



<p>(51) 国際特許分類 H04L 9/08, 9/14, 9/32, H04H 1/00</p>	<p>A1</p>	<p>(11) 国際公開番号 WO99/50992</p> <p>(43) 国際公開日 1999年10月7日(07.10.99)</p>
<p>(21) 国際出願番号 PCT/JP99/01606</p> <p>(22) 国際出願日 1999年3月30日(30.03.99)</p> <p>(30) 優先権データ 特願平10/89098 1998年4月1日(01.04.98) JP 特願平10/161082 1998年6月9日(09.06.98) JP 特願平10/162667 1998年6月10日(10.06.98) JP</p> <p>(71) 出願人 (米国を除くすべての指定国について) 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.)[JP/JP] 〒571-8501 大阪府門真市大字門真1006番地 Osaka, (JP)</p> <p>(72) 発明者 ; および (75) 発明者 / 出願人 (米国についてのみ) 西村拓也(NISHIMURA, Takuya)[JP/JP] 〒545-0053 大阪府大阪市阿倍野区松崎町3-9-18-F Osaka, (JP) 飯塚裕之(IITSUKA, Hiroyuki)[JP/JP] 〒576-0033 大阪府交野市私市6-25-6 Osaka, (JP) 山田正純(YAMADA, Masazumi)[JP/JP] 〒570-0011 大阪府守口市金田町6-24-10 Osaka, (JP) 後藤昌一(GOTOH, Shoichi)[JP/JP] 〒576-0021 大阪府交野市妙見坂5-4-204 Osaka, (JP)</p>		<p>武知秀明(TAKECHI, Hideaki)[JP/JP] 〒533-0004 大阪府大阪市東淀川区小松4丁目11-10 レモンフラッツ201 Osaka, (JP)</p> <p>(74) 代理人 弁理士 松田正道(MATSUDA, Masamichi) 〒532-0003 大阪府大阪市淀川区宮原5丁目1番3号 新大阪生島ビル Osaka, (JP)</p> <p>(81) 指定国 CN, KR, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)</p> <p>添付公開書類 国際調査報告書 補正書</p>
<p>(54) Title: DATA TRANSMITTING/RECEIVING METHOD, DATA TRANSMITTER, DATA RECEIVER, DATA TRANSMITTING/RECEIVING SYSTEM, AV CONTENT TRANSMITTING METHOD, AV CONTENT RECEIVING METHOD, AV CONTENT TRANSMITTER, AV CONTENT RECEIVER, AND PROGRAM RECORDING MEDIUM</p> <p>(54) 発明の名称 データ送受信方法、データ送信装置、データ受信装置、データ送受信システム、AVコンテンツ送信方法、AVコンテンツ受信方法、AVコンテンツ送信装置、AVコンテンツ受信装置およびプログラム記録媒体</p> <p>(57) Abstract A data transmitting/receiving method ensuring a high security enhanced by control key update and a high transmission/reception efficiency enhanced by reducing the numbers of authentications and key exchanges. An STB (1) transmits encrypted digital data (Kw(D)) encrypted from digital data (D) using a work key (Kw) and an encrypted work key (Kc(Kw)) encrypted from the work key (Kw) using a control key (Kc), regularly or irregularly updates the control key (Kc), and imparts an identifier (L) for identifying the control key (Kc) to every control key (Kc). A VTR apparatus (2) decrypts the received control key (Kc(Kw)) with the control key (Kc) obtained by performing authentication and key exchange with the STB1, decrypts the received work key (Kw(D)) with the control key (Kc(Kw)), obtains the digital data (D), refers to the transmitted identifier (L) when it resumes the reception after the reception is suspended, judges whether or not the control key (Kc) is updated while the reception is suspended, performs authentication and key exchange again if the control key (Kc) is judged to be updated, and thus obtains the updated control key (Kc).</p> <div data-bbox="803 1312 1291 1659"> </div> <div data-bbox="738 1680 1380 1953"> <p>2 ... VTR APPARATUS</p> <p>11 ... ENCRYPTING MEANS</p> <p>12 ... KEY ENCRYPTING MEANS</p> <p>13 ... TRANSMISSION-SIDE AUTHENTICATING/KEY EXCHANGING MEANS</p> <p>15 ... IDENTIFIER GENERATING MEANS</p> <p>16 ... IDENTIFIER TRANSMITTING MEANS</p> <p>21 ... ENCRYPTING MEANS</p> <p>22 ... KEY RESTORING MEANS</p> <p>23 ... RECEPTION-SIDE AUTHENTICATING/KEY EXCHANGING MEANS</p> <p>25 ... IDENTIFIER RECOGNISING MEANS</p> <p>26 ... IDENTIFIER STORAGE MEANS</p> <p>27 ... IDENTIFIER REQUESTING MEANS</p> <p>A ... REQUEST</p> <p>B ... AUTHENTICATION</p> <p>C ... INSTRUCTION TO OBTAIN Kc</p> </div>		

(57)要約

コントロールキー更新によりセキュリティを高め、認証・鍵交換の回数を減らすことにより、送受信効率を高めるデータ送受信方法を提供する。STB 1は、デジタルデータDにワークキーKwを用いて暗号化した暗号化デジタルデータKw(D)と、KwにコントロールキーKcを用いて暗号化した暗号化ワークキーKc(Kw)とを送信し、Kcを定期的または不定期的に更新するとともに、Kc毎にKcを特定できる識別子Lを付与し、VTR装置2は、STB 1と認証・鍵交換を行って得たKcを用いて、受信したKc(Kw)を解読し、このKwを用いて受信したKw(D)を解読して、Dを得、受信中断後に受信を再開する際に、送信されてきたLを参照することにより、受信中断中にKcが更新されたか否かを判断し、Kcが更新されたと判断した場合には、前記認証・鍵交換を改めて行うことによって、更新後のKcを得る。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AL	アルバニア	EE	エストニア	LC	セントルシア	SD	スーダン
AM	アルメニア	ES	スペイン	LI	リヒテンシュタイン	SE	スウェーデン
AT	オーストリア	FI	フィンランド	LK	スリ・ランカ	SG	シンガポール
AU	オーストラリア	FR	フランス	LR	リベリア	SI	スロヴェニア
AZ	アゼルバイジャン	GA	ガボン	LS	レソト	SK	スロヴァキア
BA	ボスニア・ヘルツェゴビナ	GB	英国	LT	リトアニア	SL	シエラ・レオネ
BB	バルバドス	GD	グレナダ	LU	ルクセンブルグ	SN	セネガル
BE	ベルギー	GE	グルジア	LV	ラトヴィア	SZ	スワジランド
BF	ブルキナ・ファソ	GH	ガーナ	MA	モロッコ	TD	チャード
BG	ブルガリア	GM	ガンビア	MC	モナコ	TG	トーゴ
BJ	ベナン	GN	ギニア	MD	モルドヴァ	TJ	タジキスタン
BR	ブラジル	GW	ギニア・ビサウ	MG	マダガスカル	TZ	タンザニア
BY	ベラルーシ	GR	ギリシャ	MK	マケドニア旧ユーゴスラヴィア	TM	トルクメニスタン
CA	カナダ	HR	クロアチア		共和国	TR	トルコ
CF	中央アフリカ	HU	ハンガリー	ML	マリ	TT	トリニダード・トバゴ
CG	コンゴ	ID	インドネシア	MN	モンゴル	UA	ウクライナ
CH	スイス	IE	アイルランド	MR	モーリタニア	UG	ウガンダ
CI	コートジボワール	IL	イスラエル	MW	マラウイ	US	米国
CM	カメルーン	IN	インド	MX	メキシコ	UZ	ウズベキスタン
CN	中国	IS	アイスランド	NE	ニジェール	VN	ヴェトナム
CR	コスタ・リカ	IT	イタリア	NL	オランダ	YU	ユーゴスラビア
CU	キューバ	JP	日本	NO	ノルウェー	ZA	南アフリカ共和国
CY	キプロス	KE	ケニア	NZ	ニュージーランド	ZW	ジンバブエ
CZ	チェッコ	KG	キルギスタン	PL	ポーランド		
DE	ドイツ	KP	北朝鮮	PT	ポルトガル		
DK	デンマーク	KR	韓国	RO	ルーマニア		

明 細 書

データ送受信方法、データ送信装置、データ受信装置、データ送受信システム、ＡＶコンテンツ送信方法、ＡＶコンテンツ受信方法、ＡＶコンテンツ送信装置、ＡＶコンテンツ受信装置およびプログラム記録媒体

技術分野

本発明は、データ送受信方法、データ送信装置、データ受信装置、データ送受信システムおよび前記各装置に備えられた手段の機能の全部または一部をコンピュータに実行させるプログラムを格納する媒体に関するものである。

また、本発明は、異なる暗号化手法で暗号化されたＡＶコンテンツの送信と、そのＡＶコンテンツの受信とに関するものである。

背景技術

従来技術として、第１の従来技術と、第２の従来技術とがあるので、それぞれを順番に説明する。

先ず、第１の従来技術を述べる。特定のユーザー、特定の機器等に対してのみ、データを提供する場合、提供対象以外の人間、機器に当該データを利用できなくする方法として、送信側がデータを暗号化して送信し、受信側が暗号化されたデータを解読して使用方法がある。

上記の方法について、衛星放送のＳＴＢ（Ｓｅｔ　Ｔｏｐ　Ｂｏｘ；衛星放送受信機）から当該衛星放送データを録画するＶＴＲ装置へのデータの送受信方法を例にとって、以下に説明する。本方法は、衛星放送の録画契約の対象となっているＶＴＲ装置にのみ、正しい衛星放送データを録画させるた

めに、暗号化を行うものである。

図14は、衛星放送のSTBをデータ送信装置とし、VTR装置をデータ受信装置とした場合の従来のデータ送受信システムを示す構成図である。なお、本構成図は、STBとVTR装置とのデータの送受信に関する構成要素のみを示したものであり、STBにおける衛星からの受信手段等、VTR装置における記録媒体への記録手段等については、図示を省略している。本システムは、衛星から受信した電波をAVデータに変換して、VTR装置102へ送信するSTB101、STB101から送信されてきた前記AVデータを記録媒体に記録するVTR装置102から構成されている。

STB101は、ワークキーKwを定期的または不定期的に更新生成し、衛星から受信した電波をAVデータに変換して得られたデジタルデータDに、ワークキーKwを用いて第1の暗号化を施して暗号化デジタルデータKw(D)に変換して、VTR装置102へ送信する暗号化手段111と、コントロールキーKcを生成し、ワークキーKwにコントロールキーKcを用いて第2の暗号化を施して暗号化ワークキーKc(Kw)に変換して、VTR装置102へ送信する鍵暗号化手段112と、VTR装置102との認証・鍵交換を行う送信側認証・鍵交換手段113と、VTR装置102のD-I/F124と直接データの伝達を行うD-I/F(デジタルインターフェイス)114とを備えている。

VTR装置102は、STB101のD-I/F114と直接データの伝達を行うD-I/F124と、STB101の送信側認証・鍵交換手段113との認証・鍵交換を行う受信側認証・鍵交換手段123と、暗号化ワークキーKc(Kw)を、受信側認証・鍵交換手段123を介して得られたコン

トロールキーK_cを用いて解読して、ワークキーK_wを復元する鍵復元手段122と、暗号化デジタルデータK_w(D)を、鍵復元手段122によって復元されたワークキーK_wを用いて解読して、デジタルデータDを復元する暗号解読手段121とを備えている。

STB101からVTR装置102へ送信されるデータは、暗号化デジタルデータK_w(D)、暗号化ワークキーK_c(K_w)およびコントロールキーK_cであるが、暗号化デジタルデータK_w(D)および暗号化ワークキーK_c(K_w)は、暗号化されたデータであり、コントロールキーK_cは、送信側認証・鍵交換手段113と受信側認証・鍵交換手段123との間で認証を行った後に、送信されるものであるから、不正にデータを利用しようとする第三者に対しては、セキュリティの高いシステムとなっている。

次に、第2の従来技術を述べる。上述したように、近年、映画等のAVコンテンツ(AVデータ)をデジタル信号を用いて送信し、そのAVコンテンツを受信するといったことに関する技術が進歩してきている。

そのようなAVコンテンツを送信する送信装置は、AVコンテンツを送信する前に、内容を保護するという目的のために、AVコンテンツの暗号化を行う。そして、受信装置は、暗号化されたAVコンテンツを受信し解読して、そのAVコンテンツの内容をモニタに表示する。

さて、上述したように、送信装置はAVコンテンツを暗号化するが、その暗号化に用いる暗号化手法には、複数の種類がある。例えば、受信装置がテレビ等の通常の家電機器であれば、そのような家電機器に対応させて、M6、Blowfish等の'baseline cipher'と呼ばれる「基本暗号化手法」が用いられる。それに対して、例えば、受信装置がパソコン等の演算能力の高い機器

であれば、DES等の暗号の強度がより高く、より複雑な「拡張暗号化手法」が用いられる。

従来技術と同様に、課題も第1の従来技術と、第2の従来技術とにそれぞれ対応して存在するので、それぞれの課題を順番に説明する。

まず、第1の従来技術に対する課題を述べる。上述したように、コントロールキーKcは、認証を行った後送信されるものであるが、同じKcをずっと使用していると、第三者によってKcが解読されてしまう可能性が高くなるため、Kcを定期的または不定期的に更新することによって、よりセキュリティの高いシステムとすることが考えられるが、Kcの更新の度に認証・鍵交換を実行する必要があるため、システムに与える負荷を低減し、送受信効率を高めるという観点から、認証・鍵交換の回数をできるだけ減らすことが求められている。

図15は、従来のデータ送受信システムにおいて、コントロールキーを更新するとした場合の、コントロールキー更新と認証・鍵交換の実行の関係を示す模式図である。図の横方向は、時間の経過を表し、一段目の帯は、STBがデータ信号を送信中であることを示す。2段目の矢印は、同じコントロールキーKcが使用されている範囲を示し、本図では途中でKc[1]からKc[2]に更新されたことを示している。3～5段目の帯は、各ケースにおけるVTR装置が受信状態であることを示し、帯が途切れている範囲は、受信が中断状態であることを示す。また、3～5段目の縦向きの両矢印は、認証・鍵交換が実行されたことを示す。

ケース1のVTR装置は、受信開始後に受信中断がないため、受信開始時に認証・鍵交換を実行し、以後は、コントロールキーKcの更新時のみに認

証・鍵交換を実行するだけでよい。ケース2およびケース3のVTR装置は、受信開始後に受信中断が起こったため、受信再開時に認証・鍵交換を実行しなければならない。特に、ケース3のVTR装置においては、中断時間が短かったため、受信再開時にKcが更新されていないにも関わらず、改めて認証・鍵交換を実行しなければならない、他のケースに比べてトータルの認証・鍵交換の実行回数が増えることとなる。

本発明は、上述した従来のデータ送受信方法およびデータ送受信システムの課題を考慮し、コントロールキー更新によりセキュリティを高め、認証・鍵交換の実行回数を減らすことによって送受信効率を高めるデータ送受信方法、データ送信装置、データ受信装置、データ送受信システムおよび、前記各装置に備えられた各構成手段の全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したプログラム記録媒体を提供することを目的とするものである。

次に、第2の従来技術に対する課題を述べる。その第2の従来技術を説明するさいに用いた送信装置がパソコン等の演算能力の高い機器であって、IEEE1394バスを利用して、AVコンテンツを送信し、そのIEEE1394バスを介して、受信装置がAVコンテンツを受信する場合、上述したように、受信装置がパソコン等の演算能力の高い機器であれば、送信装置は「拡張暗号化手法」を使用してAVコンテンツを暗号化し送信しても、受信装置はそのAVコンテンツを解読することができるので、何等問題は起こらない。

しかしながら、図16に示すように、例えば、パソコン58という受信装置とともに、セットトップボックス（衛星放送受信機）59のような通常の

家電機器も、IEEE 1394バスを介して送信装置57に接続されている場合がある。その場合、送信装置57が「拡張暗号化手法」を使用してAVコンテンツを暗号化して送信し、パソコン58が受信し解読しているときに、その送信の途中から、セットトップボックス59がそのAVコンテンツを受信し解読しようとしても、セットトップボックス59は、「拡張暗号化手法」を使用することができないので、そのAVコンテンツを解読することができない。

発明の開示

本発明は、上述したように、AVコンテンツ送信装置が第1の暗号化手法で暗号化したAVコンテンツを送信しているときに、その第1の暗号化手法を使用することができないAVコンテンツ受信装置がそのAVコンテンツを解読することができないという課題を考慮して、AVコンテンツ送信装置が第1の暗号化手法で暗号化したAVコンテンツを送信しているときに、その第1の暗号化手法を使用することができないAVコンテンツ受信装置がそのAVコンテンツを解読することができるようにするAVコンテンツ送信方法を提供することを目的とするものである。

また、本発明は、第1の暗号化手法で暗号化したAVコンテンツを送信しているときに、その第1の暗号化手法を使用することができないAVコンテンツ受信装置がそのAVコンテンツを解読することができるようにするAVコンテンツ送信装置を提供することを目的とするものである。

また、本発明は、上述したAVコンテンツ送信方法を用いたさい、第1の暗号化手法で暗号化されたAVコンテンツを受信し解読していた、第1の暗

号化手法を使用することができないＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置がある場合、その別のＡＶコンテンツ受信装置が引き続きそのＡＶコンテンツを解読することができるようにするＡＶコンテンツ送信方法およびＡＶコンテンツ受信方法を提供することを目的とするものである。

さらに、本発明は、上述したＡＶコンテンツ送信装置が第１の暗号化手法を使用することができないＡＶコンテンツ受信装置にそのＡＶコンテンツを解読させる場合、そのＡＶコンテンツ受信装置とは別に、第１の暗号化手法で暗号化されていたＡＶコンテンツを引き続き解読するＡＶコンテンツ受信装置を提供することを目的とするものである。

上述した課題を解決するために、第１の本発明（請求項１に対応）は、送信側が、デジタルデータにワークキーを用いて第１の暗号化を施した暗号化デジタルデータと、前記ワークキーにコントロールキーを用いて第２の暗号化を施した暗号化ワークキーとを送信し、受信側が、前記送信側と認証・鍵交換を行うことによって得た前記コントロールキーを用いて、受信した前記暗号化ワークキーを解読し、解読して得られた前記ワークキーを用いて受信した前記暗号化デジタルデータを解読して、前記デジタルデータを得るデータ送受信方法において、前記送信側は、前記コントロールキーを定期的または不定期的に更新するとともに、前記コントロールキー毎に前記コントロールキーを特定できる識別子を付与し、前記受信側は、受信中断後に受信を再開する際に、前記送信側から送信されてきた前記識別子を参照することにより、前記受信中断中に前記コントロールキーが更新されたか否かを判断し、前記コントロールキーが更新されたと判断した場合には、前記認証・鍵交換を改めて行うことによって、更新後の前記コントロールキーを得る

ことを特徴とするデータ送受信方法である。

第2の本発明（請求項6に対応）は、ワークキーを定期的または不定期的に更新生成し、デジタルデータに前記ワークキーを用いて第1の暗号化を施して暗号化デジタルデータに変換して、データ受信装置へ送信する暗号化手段と、

コントロールキーを定期的または不定期的に更新生成し、前記ワークキーに前記コントロールキーを用いて第2の暗号化を施して暗号化ワークキーに変換して、前記データ受信装置へ送信する鍵暗号化手段と、

前記データ受信装置との認証・鍵交換を行う送信側認証・鍵交換手段と、
前記コントロールキーを特定できる識別子を生成する識別子生成手段と、
前記識別子を前記データ受信装置へ送信する識別子送信手段とを
備えたことを特徴とするデータ送信装置である。

第3の本発明（請求項8に対応）は、データ送信装置との認証・鍵交換を行う受信側認証・鍵交換手段と、

ワークキーにコントロールキーを用いて第2の暗号化を施して変換された暗号化ワークキーを、前記受信側認証・鍵交換手段を介して得られた前記コントロールキーを用いて解読して、前記ワークキーを復元する鍵復元手段と

、
デジタルデータに前記ワークキーを用いて第1の暗号化を施して変換された暗号化デジタルデータを、前記鍵復元手段によって復元された前記ワークキーを用いて解読して、前記デジタルデータを復元する暗号解読手段と、

少なくとも、受信中断後に受信を再開する際に、前記データ送信装置から

送信されてきた、前記コントロールキーを特定するための識別子を参照することにより、前記コントロールキーが更新されたか否かを判断し、前記コントロールキーが更新されたと判断した場合には、前記受信側認証・鍵交換手段に前記認証・鍵交換を改めて行って更新後の前記コントロールキーを得ることを指示する識別子認識手段とを

備えたことを特徴とするデータ受信装置である。

第4の本発明（請求項1.4に対応）は、本発明のデータ送信装置および本発明のデータ受信装置を備えたことを特徴とするデータ送受信システムである。

第5の本発明（請求項1.5に対応）は、本発明のデータ送信装置およびデータ受信装置が備える各構成手段の全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体である。

第6の本発明（請求項1.6に対応）は、AVコンテンツ送信装置が伝送路を利用して第1の暗号化手法で暗号化したAVコンテンツを送信しているときに、

その第1の暗号化手法を使用することができないAVコンテンツ受信装置から認証要求があると、

その認証要求をしたAVコンテンツ受信装置が使用することができる第2の暗号化手法で前記AVコンテンツを暗号化して送信する

ことを特徴とするAVコンテンツ送信方法である。

第7の本発明（請求項1.7に対応）は、第6の本発明のAVコンテンツ送信方法において、

前記認証要求があったさい、既にそれまでの前記第 1 の暗号化手法で暗号化された A V コンテンツを受信し解読していた、前記認証要求をした A V コンテンツ受信装置とは別の A V コンテンツ受信装置がある場合、

その別の A V コンテンツ受信装置に、暗号化手法が前記第 2 の暗号化手法に切り替わることを通知する

ことを特徴とする A V コンテンツ送信方法である。

第 8 の本発明（請求項 1 8 に対応）は、第 7 の本発明の A V コンテンツ送信方法において、前記暗号化手法の切り替えを、所定のコマンドを用いて、または前記 A V コンテンツのなかに付加して通知することを特徴とする A V コンテンツ送信方法である。

第 9 の本発明（請求項 1 9 に対応）は、第 8 の本発明の A V コンテンツ送信方法において、前記切り替えた後の前記第 2 の暗号化手法がどのような暗号化手法であるのかという情報を、所定のコマンドを用いて、または前記 A V コンテンツのなかに付加して通知することを特徴とする A V コンテンツ送信方法である。

第 1 0 の本発明（請求項 2 0 に対応）は、第 8 の本発明の A V コンテンツ送信方法において、前記切り替えた後の前記第 2 の暗号化手法で使用する暗号化鍵またはその暗号化鍵の種を、所定のコマンドを用いて、または前記 A V コンテンツのなかに付加して通知することを特徴とする A V コンテンツ送信方法である。

第 1 1 の本発明（請求項 2 1 に対応）は、第 6 の本発明の A V コンテンツ送信方法において、前記暗号化手法の切り替えのタイミングを、前記認証要求がある前に使用していた前記第 1 の暗号化手法での暗号化鍵の更新のタイ

ミングとすることを特徴とするAVコンテンツ送信方法である。

第12の本発明（請求項22に対応）は、第7の本発明のAVコンテンツ送信方法において、少なくとも前記別のAVコンテンツ受信装置に、前記暗号化手法が前記第2の暗号化手法に切り替わることを通知するとともに、その暗号化手法の切り替えのタイミングの情報を送信することを特徴とするAVコンテンツ送信方法である。

第13の本発明（請求項23に対応）は、第6の本発明のAVコンテンツ送信方法において、

前記AVコンテンツ送信装置が前記認証要求をしたAVコンテンツ受信装置を記憶し、

そのAVコンテンツ受信装置から、前記AVコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドが来ているか否かを判断し、前記コマンドが来なくなった場合、

前記暗号化手法を前記第2の暗号化手法から前記第1の暗号化手法に切り替える

ことを特徴とするAVコンテンツ送信方法である。

第14の本発明（請求項24に対応）は、第6の本発明のAVコンテンツ送信方法において、

前記AVコンテンツ送信装置が、前記認証要求をしたAVコンテンツ受信装置と前記そのAVコンテンツ受信装置とは別のAVコンテンツ受信装置とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、

前記AVコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を

要求するコマンドを送信してくるＡＶコンテンツ受信装置が、全て前記第１の暗号化手法を使用することができるＡＶコンテンツ受信装置である場合、前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替える

ことを特徴とするＡＶコンテンツ送信方法である。

第１５の本発明（請求項２５に対応）は、第６から第１４のいずれかの本発明のＡＶコンテンツ送信方法の各ステップの全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体である。

第１６の本発明（請求項２６に対応）は、第６から第１４のいずれかの本発明のＡＶコンテンツ送信方法によって送信されてくるＡＶコンテンツを受信し、

そのＡＶコンテンツが暗号化されたさいに使用された暗号化手法に基づくとともに、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種を利用して、前記暗号化されたＡＶコンテンツを解読する

ことを特徴とするＡＶコンテンツ受信方法である。

第１７の本発明（請求項２７に対応）は、第１６の本発明のＡＶコンテンツ送信方法において、

第６から第１４のいずれかの本発明のＡＶコンテンツ送信方法によって送信されてくるＡＶコンテンツとともに、またはそのＡＶコンテンツのなかに、前記暗号化手法の切り替えに関する情報があって、

その情報に、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵

の種との一方または両方が含まれていない場合、

前記ＡＶコンテンツ送信装置に対して、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種とのうちの前記暗号化手法の切り替えに関する情報に含まれていないものを送信するように要求する

ことを特徴とするＡＶコンテンツ受信方法である。

第１８の本発明（請求項２８に対応）は、第１６または第１７の本発明のＡＶコンテンツ受信方法の各ステップの全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体である。

第１９の本発明（請求項２９に対応）は、送信しようとするＡＶコンテンツを暗号化するさいの暗号化手法を選択する暗号化手法選択手段と、

その暗号化手法選択手段によって選択された暗号化手法に対応した、ＡＶコンテンツを暗号化するための暗号化鍵を生成する暗号化鍵生成手段と、

ＡＶコンテンツを入力するとともに、前記暗号化鍵生成手段からの前記暗号化鍵を入力し、その暗号化鍵を利用して、前記ＡＶコンテンツを暗号化する暗号化手段と、

ＡＶコンテンツ受信装置との間で認証・鍵交換を行う送信側認証・鍵交換手段とを備え、

ＡＶコンテンツ送信装置が、前記暗号化手法選択手段によって選択された第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、

その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置から認証要求があると、前記送信側認証・鍵交換手段が、その認証要求をし

たAVコンテンツ受信装置との間で認証を行い、

前記暗号化手法選択手段が、暗号化手法を、前記認証要求をしたAVコンテンツ受信装置が使用することができる第2の暗号化手法に切り替えることを特徴とするAVコンテンツ送信装置である。

第20の本発明（請求項30に対応）は、第19の本発明のAVコンテンツ送信装置において、

前記認証要求があったさい、既にそれまでの前記第1の暗号化手法で暗号化されたAVコンテンツを受信し解読していた、前記認証要求をしたAVコンテンツ受信装置とは別のAVコンテンツ受信装置がある場合、

その別のAVコンテンツ受信装置に、暗号化手法が前記第2の暗号化手法に切り替わることを通知する暗号化手法通知手段を備えた

ことを特徴とするAVコンテンツ送信装置である。

第21の本発明（請求項31に対応）は、第19の本発明のAVコンテンツ送信装置において、

前記暗号化鍵生成手段が、定期的または不定期に前記暗号化鍵を更新し、

前記暗号化手法選択手段が暗号化手法を前記第2の暗号化手法に切り替えるタイミングが、前記暗号化鍵生成手段が前記第1の暗号化手法において暗号化鍵を更新するタイミングである

ことを特徴とするAVコンテンツ送信装置である。

第22の本発明（請求項32に対応）は、第19の本発明のAVコンテンツ送信装置において、

前記送信側認証・鍵交換手段が、前記認証要求をしたAVコンテンツ受信装置を記憶するとともに、そのAVコンテンツ受信装置から、前記AVコン

テンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドが来ているか否かを判断し、前記コマンドが来なくなったと判断した場合

、
前記暗号化手法選択手段が、前記暗号化手法を前記第2の暗号化手法から前記第1の暗号化手法に切り替える

ことを特徴とするAVコンテンツ送信装置である。

第23の本発明（請求項33に対応）は、第19の本発明のAVコンテンツ送信装置において、

前記送信側認証・鍵交換手段が、前記認証要求をしたAVコンテンツ受信装置と前記そのAVコンテンツ受信装置とは別のAVコンテンツ受信装置とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、

前記AVコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドを送信してくるAVコンテンツ受信装置が、全て前記第1の暗号化手法を使用することができるAVコンテンツ受信装置である場合、

前記暗号化手法選択手段が、前記暗号化手法を前記第2の暗号化手法から前記第1の暗号化手法に切り替える

ことを特徴とするAVコンテンツ送信装置である。

第24の本発明（請求項34に対応）は、第19から第23のいずれかの本発明のAVコンテンツ送信装置との間で認証・鍵交換を行う受信側認証・鍵交換手段と、

前記AVコンテンツ送信装置からの暗号化されたAVコンテンツのその暗号化に利用された暗号化手法の情報を入力し、記憶する暗号化手法記憶手段

と、

前記ＡＶコンテンツ送信装置からの暗号化されたＡＶコンテンツを入力するとともに、前記ＡＶコンテンツ送信装置からの暗号化鍵またはその暗号化鍵の種を入力し、その後、前記暗号化手法記憶手段に記憶されている暗号化手法に基づき、かつ、前記暗号化鍵またはその暗号化鍵の種を利用して、前記暗号化されたＡＶコンテンツを解読する暗号解読手段とを備えた

ことを特徴とするＡＶコンテンツ受信装置である。

第２５の本発明（請求項３５に対応）は、第２４の本発明のＡＶコンテンツ受信装置において、

第１９から第２３のいずれかの本発明のＡＶコンテンツ送信装置から送信されてくるＡＶコンテンツとともに、またはそのＡＶコンテンツのなかに、前記暗号化手法の切り替えに関する情報があつて、

その情報に、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種との一方または両方が含まれていない場合、

前記ＡＶコンテンツ送信装置に対して、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種とのうちの前記情報に含まれていないものを送信するように要求する要求手段を備えた

ことを特徴とするＡＶコンテンツ受信装置である。

図面の簡単な説明

図１は、本発明の第１の実施の形態におけるデータ送受信システムの構成

を示す構成図である。

図2は、本発明の第1の実施の形態におけるデータ送受信システムにおいて、STB1がデータを暗号化して送信し、VTR装置2が暗号化されたデータを解読して使用方法の手順を示すフロー図である。

図3は、本発明の第1の実施の形態におけるデータ送受信システムにおいて、受信中断が生じ、受信を再開する場合の手順を示すフロー図である。

図4は、本発明の第1の実施の形態におけるデータ送受信システムのコントロールキー更新と認証・鍵交換の実行の関係を示す模式図である。

図5は、本発明の第2の実施の形態におけるデータ送受信システムの構成を示す構成図である。

図6は、本発明の第2の実施の形態におけるデータ送受信システムにおいて、STB1がデータを暗号化して送信し、VTR装置2が暗号化されたデータを解読して使用方法の手順を示すフロー図である。

図7は、本発明の第2の実施の形態におけるデータ送受信システムにおいて、受信中断が生じ、受信を再開する場合の手順を示すフロー図である。

図8は、本発明の第2の実施の形態におけるデータ送受信システムのコントロールキー更新と認証・鍵交換の実行の関係を示す模式図である。

図9は、本発明の第3の実施の形態のAVコンテンツ通信システムのブロック図である。

図10は、本発明の第3の実施の形態のAVコンテンツ通信システムのAVコンテンツ送信装置31が送信するAVコンテンツおよびコマンドを含むデータの構成図である。

図11は、本発明の第3の実施の形態のAVコンテンツ通信システムのA

Vコンテンツ送信装置31の動作の一部を示すフローチャートである。

図12は、本発明の第3の実施の形態のAVコンテンツ通信システムの第1のAVコンテンツ受信装置32の動作の一部を示すフローチャートである。

図13は、図11とは異なる、本発明の第3の実施の形態のAVコンテンツ通信システムのAVコンテンツ送信装置31の動作の一部を示すフローチャートである。

図14は、従来のデータ送受信システムを示す構成図である。

図15は、従来のデータ送受信システムにおいて、コントロールキーを更新するとした場合の、コントロールキー更新と認証・鍵交換の実行の関係を示す模式図である。

図16は、第2の従来技術の課題を説明するための図である。

(符号の説明)

- 1、101 STB
- 2、102 VTR装置
- 11、111 暗号化手段
- 12、112 鍵暗号化手段
- 13、113 送信側認証・鍵交換手段
- 14、24、114、124 D-I/F
- 15 識別子生成手段
- 16 識別子送信手段
- 21、121 暗号解読手段
- 22、122 鍵復元手段
- 23、123 受信側認証・鍵交換手段

- 25 識別子認識手段
- 26 識別子記憶手段
- 27 識別子要求手段
- 31 AVコンテンツ送信装置
- 32 第1のAVコンテンツ受信装置
- 33 第2のAVコンテンツ受信装置
- 34 アンテナ
- 35、36 モニタ
- 37 受信手段
- 38 暗号化手段
- 39 Kco生成手段
- 40 暗号化手法選択手段
- 41、46、53 AKE手段
- 42 暗号化手法変更通知手段
- 43 Kco要求コマンド応答手段
- 44、45、52 データ転送手段
- 47 暗号化手法通知検出手段
- 48、54 Kco要求コマンド発行手段
- 49、55 Kco記憶手段
- 50 暗号化手法記憶手段
- 51、56 暗号解読手段
- 57 送信装置
- 58 パソコン

59 セットトップボックス（衛星放送受信機）

発明を実施するための最良の形態

以下に、本発明の実施の形態を図面を参照して説明する。

（第1の実施の形態）

以下に、本発明の第1の実施の形態を図面を参照して説明する。

図1は、本発明の第1の実施の形態におけるデータ送受信システムの構成を示す構成図である。なお、本構成図は、STBとVTR装置とのデータの送受信に関する構成要素のみを示したものであり、STBにおける衛星からの受信手段等、VTR装置における記録媒体への記録手段等については、図示を省略している。本実施の形態におけるデータ送受信システムは、衛星放送のSTBから当該衛星放送データを録画するVTR装置へデータの送受信を行うシステムであり、本発明のデータ送信装置に対応するSTB1と、本発明のデータ受信装置に対応するVTR装置2とから構成されている。

STB1は、ワークキー K_w を定期的または不定期的に更新生成し、衛星から受信した電波をAVデータに変換して得られたデジタルデータDに、ワークキー K_w を用いて第1の暗号化を施して暗号化デジタルデータ K_w (D)に変換して、VTR装置2へ送信する暗号化手段11と、コントロールキー K_c を定期的または不定期的に更新生成し、ワークキー K_w にコントロールキー K_c を用いて第2の暗号化を施して暗号化ワークキー K_c (K_w)に変換して、VTR装置2へ送信する鍵暗号化手段12と、VTR装置2との認証・鍵交換を行う送信側認証・鍵交換手段13と、VTR装置2のD

ー I / F 2 4 と直接データの伝達を行う D - I / F (デジタルインターフェイス) 1 4 と、コントロールキー K c を特定できる識別子 L を生成する識別子生成手段 1 5 と、識別子 L を V T R 装置 2 へ送信する識別子送信手段 1 6 とを備えている。

V T R 装置 2 は、S T B 1 の D - I / F 1 4 と直接データの伝達を行う D - I / F 2 4 と、S T B 1 の送信側認証・鍵交換手段 1 3 との認証・鍵交換を行う受信側認証・鍵交換手段 2 3 と、暗号化ワークキー K c (K w) を、受信側認証・鍵交換手段 2 3 を介して得られたコントロールキー K c を用いて解読して、ワークキー K w を復元する鍵復元手段 2 2 と、暗号化デジタルデータ K w (D) を、鍵復元手段 2 2 によって復元されたワークキー K w を用いて解読して、デジタルデータ D を復元する暗号解読手段 2 1 と、少なくとも、受信中断後に受信を再開する際に、S T B 1 から送信されてきた、コントロールキー K c を特定するための識別子 L を参照することにより、コントロールキー K c が更新されたか否かを判断し、コントロールキー K c が更新されたと判断した場合には、受信側認証・鍵交換手段 2 3 に前記認証・鍵交換を改めて行って更新後のコントロールキー K c を得ることを指示する識別子認識手段 2 5 と、送信されてきた識別子 L を記憶する識別子記憶手段 2 6 と、前記受信中断後に受信を再開する際に、識別子 L を送信することを S T B 1 の識別子送信手段 1 6 に対して要求する識別子要求手段 2 7 とを備えている。

なお、D - I / F 1 4 および 2 4 の具体例としては、I E E E 1 3 9 4 の D - I / F が挙げられる。これは、リアルタイム性の保証が必要となる映像や音声の様なデータの転送に適したアイソクロナス転送と、その必要のない

認証用データやコマンド等の転送に適したアシンクロナス転送の2つの転送を行うものである。

次に、本システムにおいて、STB1がデータを暗号化して送信し、VTR装置2が暗号化されたデータを解読して使用方法の手順について、図2、図3を用いて説明する。

まず、通常の送受信時の手順を図2を用いて説明する。図2は、本発明の第1の実施の形態におけるデータ送受信システムにおいて、STB1がデータを暗号化して送信し、VTR装置2が暗号化されたデータを解読して使用方法の手順を示すフロー図である。なお、図2において、左側に、STB1で行われる処理が、右側に、VTR装置2で行われる処理が示されている。また、STB1とVTR装置2との間のデータの送受信は、全てD-I/F14および24を介して行われるが、以下の説明においては、この説明を省略する。

鍵暗号化手段12は、送信開始と同時にコントロールキーKcを生成し（ステップS1）、これを送信側認証・鍵交換手段13および識別子生成手段15に送る。識別子生成手段15は、このKcを特定するための識別子Lを生成して、識別子送信手段16へ送る（ステップS2）。送信側認証・鍵交換手段13は、このKcをVTR装置2に送信するために、受信側認証・鍵交換手段23との認証・鍵交換を行う（ステップS3、S4）。このとき、識別子送信手段16は、送信されるKcに対応するLを識別子認識手段25へ送信する。VTR装置2側では、受信側認証・鍵交換手段23は、受信したKcを鍵復元手段22へ送り、識別子認識手段25は、受信したLを識別子記憶手段26に送り、記憶させる（ステップS5）。このとき、識別子記

憶手段 26 は、記憶していた古い L に上書き記憶するものとする。

一方、STB 1 側においては、暗号化手段 11 がワークキー Kw を生成し（ステップ S6）、これを鍵暗号化手段 12 へ送る。鍵暗号化手段 12 は、Kw にステップ S1 で生成されたコントロールキー Kc を用いて第 2 の暗号化を施して暗号化ワークキー Kc (Kw) に変換して、鍵復元手段 22 へ送信する（ステップ S7）。VTR 装置 2 側では、鍵復元手段 22 は、ステップ S4 において受信側認証・鍵交換手段 23 が受信した Kc を用いて、鍵暗号化手段 12 から送信されてきた Kc (Kw) を解読して、ワークキー Kw を復元して、暗号解読手段 21 へ送る（ステップ S8）。

また、STB 1 側においては、暗号化手段 11 が、衛星から受信した電波を AV データに変換して得られたデジタルデータ D に、ステップ S6 において生成したワークキー Kw を用いて第 1 の暗号化を施して暗号化デジタルデータ Kw (D) に変換して、暗号解読手段 21 へ送信する（ステップ S9）。VTR 装置 2 側では、暗号解読手段 21 は、ステップ S8 において復元された Kw を用いて、受信した Kw (D) を解読して、デジタルデータ D を復元する（ステップ S10）。

VTR 装置 2 側で、何らかの原因により受信中断が生じ、受信を再開する場合は、図 3 の A に進み、受信中断が起こらない場合は、ステップ S12 へ進む（ステップ S11）。受信を終了しない場合は、ステップ S13 へ進む（ステップ S12）。なお、受信中断が生じ、受信を再開する場合については、追って説明する。

ステップ S9 において、1 ユニットのデータの送信が終了すると、次のユニットに対してワークキー Kw の更新を行うかどうかの判断を行い（ステッ

プS 1 3)、行う場合は、ステップS 6に進んで、以下は、上記と同様の手順の処理を行う。Kwの更新を行わない場合は、コントロールキーKcの更新を行うかどうかの判断を行い(ステップS 1 4)、行う場合は、ステップS 1に進んで、以下は、上記と同様の手順の処理を行う。ただし、Kcの更新を行って、Kwの更新を行わない場合も存在するので、この場合は、ステップS 6は、省略される。Kcの更新を行わない場合、送信を終了する以外は、ステップS 9に進んで(ステップS 1 5)、以下は、上記と同様の手順の処理を行う。

次に、受信中断が生じ、受信を再開する場合の手順を図3を用いて説明する。図3は、本発明の第1の実施の形態におけるデータ送受信システムにおいて、受信中断が生じ、受信を再開する場合の手順を示すフロー図である。なお、図3においても、図2の場合と同様に、左側に、STB1で行われる処理が、右側に、VTR装置2で行われる処理が示されている。また、図2の場合と同様に、STB1とVTR装置2との間のデータの送受信は、全てD-I/F14および24を介して行われるが、以下の説明においても、この説明を省略する。

図2のステップS 1 1において、受信中断が生じ、受信を再開する場合には、識別子要求手段27は、識別子送信手段16に対して、識別子Lを送信することを要求する(ステップS 1 6)。識別子送信手段16は、この要求を受けて、Lを識別子認識手段25へ送信する(ステップS 1 7)。識別子認識手段25は、送信されてきたLと、ステップS 5において、識別子記憶手段26に記憶されたLとを比較して、送信されてきたLが記憶されていたLと異なる場合は、図2のステップS 4に進み、等しい場合は、図2のステ

ップS 8に進む（ステップS 1 8、S 1 9）。ステップS 4に進むと、識別子認識手段2 5の指示により、受信側認証・鍵交換手段2 3は、送信側認証・鍵交換手段1 3と認証・鍵交換を行うことによって、送信されてきたLに対応するコントロールキーK cを入手し（ステップS 4）、以下は図2と同様の手順の処理を行う。また、ステップS 8に進むと、K c入手に関する手続は行われず、鍵復元手段2 2は、受信中断前に使用していた、記憶されていたLに対応するK cを用いて、暗号化ワークキーK c（K w）を解読して、ワークキーK wを復元する（ステップS 8）。以下は図2と同様の手順の処理を行う。

すなわち、識別子Lについては、暗号化等の措置を施さずに送受信を行えるため、システムに与える負荷が高い認証・鍵交換の実行を行う前に、識別子Lの送受信を行い、識別子Lにしたがって、コントロールキーK cが更新されたか否かを判断し、更新されていた場合にのみ、認証・鍵交換の実行を行うことによって、システムに与える負荷を低減するものである。

図4は、本発明の第1の実施の形態におけるデータ送受信システムのコントロールキー更新と認証・鍵交換の実行の関係を示す模式図である。図の横方向は、時間の経過を表し、一段目の帯は、S T Bがデータ信号を送信中であることを示す。2段目の矢印は、同じコントロールキーK cが使用されている範囲を示し、本図では途中でK c [1] からK c [2] に更新されたことを示している。3～5段目の帯は、各ケースにおけるV T R装置が受信状態であることを示し、帯が途切れている範囲は、受信が中断状態であることを示す。また、3～5段目の縦向きの両矢印は、認証・鍵交換が実行されたことを、上向き矢印は、識別子要求手段2 7が、識別子送信手段1 6に対し

て、識別子Lを送信することを要求したことを、下向き矢印は、識別子送信手段16が識別子Lを送信したことをそれぞれ示す。

ケース1のVTR装置は、受信開始後に受信中断がないため、従来例と同様に、受信開始時に認証・鍵交換を実行し、以後は、コントロールキーKcの更新時のみに認証・鍵交換を実行するだけでよい。ケース2のVTR装置については、従来例と同様に、受信開始後に受信中断が起こり、コントロールキーKcの更新後に受信を再開したため、このことを識別子Lの送信により確認し、従来例と同様に、改めて認証・鍵交換を実行しなければならない。ケース3のVTR装置においては、中断時間が短かったため、受信再開時にKcが更新されていないので、このことを識別子Lの送信により確認し、改めて認証・鍵交換を実行することなく、受信中断前のコントロールキーKcを用いて鍵復元作業を継続することができるものである。すなわち、本実施の形態におけるデータ送受信システムは、ケース3の場合に、従来例に比べて、システムに与える負荷が高い認証・鍵交換の実行回数を減らすことができるものである。

(第2の実施の形態)

以下に、本発明の第2の実施の形態を図面を参照して説明する。本実施の形態が上述した第1の実施の形態と異なる点は、本発明のデータ受信装置が本発明の識別子要求手段を備えていない点に関する点である。したがって、本実施の形態において、第1の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第1の実施の形態と同じとする。

図5は、本発明の第2の実施の形態におけるデータ送受信システムの構成

を示す構成図である。本実施の形態におけるデータ送受信システムの構成が、図1の第1の実施の形態におけるデータ送受信システムの構成と異なるのは、VTR装置2が、識別子要求手段27を備えていないこと、STB1の暗号化手段11がコントロールキーKcの更新が行われた後、更新されたコントロールキーKcに対しての認証・鍵交換が完了するまでの間は、ワークキーKwの更新を行わないこと、および、STB1の識別子送信手段16が、定期的または不定期的に、識別子LをVTR装置2へ送信する機能を有することである。

なお、本実施の形態においては、識別子送信手段16が識別子LをVTR装置2へ送信するタイミングは、ワークキーKwが更新生成される度であり、更新生成されたワークキーKwに対応する暗号化ワークキーKc（Kw）と同時に、そのときのコントロールキーKcに対応する識別子Lを送信するものとする。しかし、これに限るものではなく、送信のタイミングは、定期的または不定期的で、Kcの更新をもれなくVTR装置2へ送信できる程度に頻繁であればよい。

次に、本システムにおいて、STB1がデータを暗号化して送信し、VTR装置2が暗号化されたデータを解読して使用方法の手順について、図6、図7を用いて説明する。

まず、通常の送受信時の手順を図6を用いて説明する。図6は、本発明の第2の実施の形態におけるデータ送受信システムにおいて、STB1がデータを暗号化して送信し、VTR装置2が暗号化されたデータを解読して使用方法の手順を示すフロー図である。通常の送受信時の手順について、第1の実施の形態において説明した図2のステップS1～S15と異なる点は

、ステップS 7において、鍵暗号化手段1 2が暗号化ワークキーK_c (K_w)を鍵復元手段2 2へ送信する際に、識別子送信手段1 6が、送信されるK_cに対応するLを識別子認識手段2 5へ送信し、ステップS 8において、識別子認識手段2 5が、受信したLを識別子記憶手段2 6に送り、記憶させることである。その他は、第1の実施の形態と同様であるため、説明を省略する。

次に、受信中断が生じ、受信を再開する場合の手順を図7を用いて説明する。図7は、本発明の第2の実施の形態におけるデータ送受信システムにおいて、受信中断が生じ、受信を再開する場合の手順を示すフロー図である。なお、図7においては、特に説明のないものについては、図3の場合と同様とする。

図6のステップS 1 1において、受信中断が生じ、受信を再開する場合には、VTR装置2側からの積極的な処理は行わず、STB 1からのデータの送付を待つ。前述したステップS 7と同様に、鍵暗号化手段1 2が暗号化ワークキーK_c (K_w)を鍵復元手段2 2へ送信する際に、識別子送信手段1 6が、送信されるK_cに対応するLを識別子認識手段2 5へ送信してくるので(ステップS 6 6)、識別子認識手段2 5は、送信されてきたLと、ステップS 5またはS 8において、識別子記憶手段2 6に記憶されたLとを比較して、送信されてきたLが記憶されていたLと異なる場合は、図6のステップS 4に進み、等しい場合は、図6のステップS 8に進む(ステップS 6 7、S 6 8)。ステップS 4に進むと、識別子認識手段2 5の指示により、受信側認証・鍵交換手段2 3は、送信側認証・鍵交換手段1 3と認証・鍵交換を行うことによって、送信されてきたLに対応するコントロールキーK_cを

入手し（ステップS 4）、以下は図6と同様の手順の処理を行う。また、ステップS 8に進むと、K c入手に関する手続は行われず、鍵復元手段2 2は、受信中断前に使用していた、記憶されていたLに対応するK cを用いて、暗号化ワークキーK c（K w）を解読して、ワークキーK wを復元する（ステップS 8）。以下は図6と同様の手順の処理を行う。

すなわち、識別子Lについては、暗号化等の措置を施さずに送受信を行えるため、システムに与える負荷が高い認証・鍵交換の実行を行う前に、識別子Lの送受信を行い、識別子Lにしたがって、コントロールキーK cが更新されたか否かを判断し、更新されていた場合にのみ、認証・鍵交換の実行を行うことによって、システムに与える負荷を低減するものである。

また、本実施の形態においては、S T B 1の暗号化手段1 1がコントロールキーK cの更新が行われた後、更新されたコントロールキーK cに対しての認証・鍵交換が完了するまでの間は、ワークキーK wの更新を行わないこととしているので、認証・鍵交換の途中で行われたK wの更新結果を受け取れないという不具合も防止できる。

図8は、本発明の第2の実施の形態におけるデータ送受信システムのコントロールキー更新と認証・鍵交換の実行の関係を示す模式図である。図の横方向は、時間の経過を表し、一段目の帯は、S T Bがデータ信号を送信中であることを示す。二段目の矢印は、同じコントロールキーK cが使用されている範囲を示し、本図では途中でK c [1] からK c [2] に更新されたことを示している。3～5段目の帯は、各ケースにおけるV T R装置が受信状態であることを示し、帯が途切れている範囲は、受信が中断状態であることを示す。また、3～5段目の縦向きの両矢印は、認証・鍵交換が実行された

ことを、下向き矢印は、識別子送信手段 16 が識別子 L を送信したことをそれぞれ示す。前述したように、鍵暗号化手段 12 が暗号化ワークキー K_c (K_w) を鍵復元手段 22 へ送信する際に、識別子送信手段 16 が、送信される K_c に対応する L を識別子認識手段 25 へ送信しているのです、これを示す下向き矢印が VTR 装置の受信状態に関わらず、頻繁に現れている。

ケース 1 の VTR 装置は、受信開始後に受信中断がないため、従来例と同様に、受信開始時に認証・鍵交換を実行し、以後は、コントロールキー K_c の更新時のみに認証・鍵交換を実行するだけでよい。ケース 2 の VTR 装置については、従来例と同様に、受信開始後に受信中断が起こり、コントロールキー K_c の更新後に受信を再開したため、このことを識別子 L の送信により確認し、従来例と同様に、改めて認証・鍵交換を実行しなければならない。ケース 3 の VTR 装置においては、中断時間が短かったため、受信再開時に K_c が更新されていないので、このことを識別子 L の送信により確認し、改めて認証・鍵交換を実行することなく、受信中断前のコントロールキー K_c を用いて鍵復元作業を継続することができるものである。すなわち、本実施の形態におけるデータ送受信システムは、ケース 3 の場合に、従来例に比べて、システムに与える負荷が高い認証・鍵交換の実行回数を減らすことができるものである。

なお、第 2 の実施の形態におけるデータ送受信システムのデータ送信装置は、請求項 7 の本発明の機能を有するものであるとして説明したが、本機能を有さない場合においても、認証・鍵交換の実行回数を減らすことによって、送受信効率を高めるという効果はある。また、第 1 の実施の形態におけるデータ送受信システムのデータ送信装置が、本機能を有するものであるとし

ても、第2の実施の形態におけるデータ送受信システムと同様の効果が得られる。

また、上述した第1および第2の実施の形態におけるデータ送受信システムおよびデータ受信装置は、本発明の識別子記憶手段を備えるとして説明したが、これに限るものではなく、要するに、本発明の識別子認識手段が、少なくとも、受信中断後に受信を再開する際に、データ送信装置から送信されてきた、コントロールキーを特定するための識別子を参照することにより、前記コントロールキーが更新されたか否かを判断できる構成でありさえすればよい。

また、本発明のデータ送受信方法、データ送受信システム、データ送信装置およびデータ受信装置は、上述した第1および第2の実施の形態においては、衛星放送のSTBから当該衛星放送データを録画するVTR装置へデータの送受信を行うものであるとして説明したが、これに限るものではなく、送信側がデータを暗号化して送信し、受信側が暗号化されたデータを解読して使用するものであり、暗号化に用いた鍵を、認証・鍵交換を行うことによって送信するものであればよい。

また、上述した第1および第2の実施の形態においては、本発明のデータ送受信システムを中心に説明したが、本発明のデータ送受信方法は、上記説明中で、説明された方法である。また、本発明のプログラム記録媒体は、上述した各方法の全部または一部の各機能をコンピュータに実行させるプログラムを格納したもの、例えば、図2および図3、または、図6および図7に記載のステップの全部または一部をコンピュータに実行させるプログラムを格納したものである。

さらに、上述した第1および第2の実施の形態におけるデータ送受信システムの各構成手段・構成要素の全部または一部は、ハードウェアであってもよいし、そのハードウェアの該当する機能と同じ機能を有するソフトウェアであってもよい。

(第3の実施の形態)

次に、本発明の第3の実施の形態のAVコンテンツ通信システムの構成を述べる。

図9に、本発明の第3の実施の形態のAVコンテンツ通信システムのブロック図を示す。図9に示すように、本発明の第3の実施の形態のAVコンテンツ通信システムは、AVコンテンツ送信装置31と、第1のAVコンテンツ受信装置32と、第2のAVコンテンツ受信装置33と、IEEE1394バスから構成される。なお、図9には、アンテナ34と、モニタ35および36も表示する。

さて、AVコンテンツ送信装置31は、図9に示すように、受信手段37と、暗号化手段38と、Kco生成手段39と、暗号化手法選択手段40と、AKE手段41と、暗号化手法変更通知手段42と、Kco要求コマンド応答手段43と、データ転送手段44から構成される。

受信手段37は、AVコンテンツを、AVコンテンツ送信装置31外部のアンテナ34を介して受信する手段である。

暗号化手段38は、基本暗号化手法と拡張暗号化手法とを使用することができるものであって、受信手段37からのAVコンテンツを入力するとともに、Kco生成手段39からの暗号化鍵Kcoを入力し、暗号化手法選択手段40によって選択された暗号化手法を使用し、暗号化鍵KcoでAVコン

テンツを暗号化する手段である。なお、暗号化鍵K c oで暗号化されたA VコンテンツをK c o (A Vコンテンツ)とする。また、基本暗号化手法と拡張暗号化手法との相違は、暗号化の強度が異なるということであって、拡張暗号化手法の方が基本暗号化手法よりも暗号化の強度が強いものであるとする。さらにいうと、暗号化するさいに用いる暗号化鍵K c oを構成するデジタル信号の長さが異なり、例えば、基本暗号化手法は、40ビットの暗号化鍵K c oを用いてA Vコンテンツを暗号化する手法であって、拡張暗号化手法は、56ビットの暗号化鍵K c oを用いてA Vコンテンツを暗号化する手法であるものとする。

K c o生成手段39は、暗号化手段38が受信手段37からのA Vコンテンツを暗号化するさいに用いる暗号化鍵K c oを生成する手段であって、その暗号化鍵K c oを20秒毎に更新するものである。

暗号化手法選択手段40は、暗号化手段38がA Vコンテンツを暗号化するさいに使用する暗号化手法を選択する手段である。

AKE手段41は、第1のA Vコンテンツ受信装置32との間で認証・鍵交換を行う手段であって、第1のA Vコンテンツ受信装置32との間で認証が成功した場合、その第1のA Vコンテンツ受信装置32に対して、交換鍵K e x (Exchange Key)を発行する手段である。また同様に、AKE手段41は、第2のA Vコンテンツ受信装置33との間で認証・鍵交換を行う手段でもある。

暗号化手法変更通知手段42は、それまでに選択していた暗号化手法からそれとは別の暗号化手法に暗号化手法の選択を変更する場合、その変更を通知する手段である。

K c o 要求コマンド応答手段 4 3 は、第 1 の A V コンテンツ受信装置 3 2 および／または第 2 の A V コンテンツ受信装置 3 3 からの、20 秒毎に更新される最新の暗号化鍵 K c o の種を送信するように要求されたコマンドを入力し、そのコマンドにしたがって暗号化鍵 K c o の種を送信する手段である。

データ転送手段 4 4 は、A V コンテンツ送信装置 3 1 の各構成手段と第 1 の A V コンテンツ受信装置 3 2 および／または第 2 の A V コンテンツ受信装置 3 3 との間でのデータ通信の仲介を行う手段である。

次に、第 1 の A V コンテンツ受信装置 3 2 は、図 9 に示すように、データ転送手段 4 5 と、A K E 手段 4 6 と、暗号化手法通知検出手段 4 7 と、K c o 要求コマンド発行手段 4 8 と、K c o 記憶手段 4 9 と、暗号化手法記憶手段 5 0 と、暗号解読手段 5 1 から構成される。

データ転送手段 4 5 は、第 1 の A V コンテンツ受信装置 3 2 の各構成手段と A V コンテンツ送信装置 3 1 との間でのデータ通信の仲介を行う手段である。

A K E 手段 4 6 は、A V コンテンツ送信装置 3 1 との間で認証・鍵交換を行う手段であって、A V コンテンツ送信装置 3 1 との間で認証が成功した場合、その A V コンテンツ送信装置 3 1 から交換鍵 K e x を入力する手段である。

暗号化手法通知検出手段 4 7 は、A V コンテンツ送信装置 3 1 からの A V コンテンツの暗号化に使用された暗号化手法がどのような暗号化手法であるのかを検出する手段である。

K c o 要求コマンド発行手段 4 8 は、暗号化手法通知検出手段 4 7 によって検出された暗号化手法にしたがって、その暗号化手法に対応する暗号化鍵

K c oの種を送信するようにA Vコンテンツ送信装置31に対して要求するコマンドを発行する手段である。また、K c o要求コマンド発行手段48は、その要求コマンドに対応する、A Vコンテンツ送信装置31からの暗号化鍵K c oの種を入力する手段でもある。

K c o記憶手段49は、あらかじめ、A Vコンテンツ送信装置31からの暗号化されたA Vコンテンツを解読するさいに必要となる所定の関数が設定されており、A K E手段46からの交換鍵K e xを入力するとともに、K c o要求コマンド発行手段48からの暗号化鍵K c oの種を入力し、交換鍵K e xと暗号化鍵K c oとをあらかじめ設定されている関数に代入して暗号化鍵K c oを生成し記憶する手段である。なお、その関数については後に述べることにする。

暗号化手法記憶手段50は、暗号化手法通知検出手段47によって検出された暗号化手法を記憶する手段である。

暗号解読手段51は、A Vコンテンツ送信装置31からの暗号化されたA Vコンテンツを入力するとともに、K c o記憶手段49からの暗号化鍵K c oと、暗号化手法記憶手段50からの暗号化手法とを入力し、その暗号化手法に基づいて、暗号化されたA Vコンテンツを暗号化鍵K c oで解読する手段である。なお、暗号解読手段51は、基本暗号化手法と拡張暗号化手法のいずれもを使用することができるものであるとする。

次に、第2のA Vコンテンツ受信装置33は、図9に示すように、データ転送手段52と、A K E手段53と、K c o要求コマンド発行手段54と、K c o記憶手段55と、暗号解読手段56から構成される。

データ転送手段52は、第2のA Vコンテンツ受信装置33の各構成手段

とAVコンテンツ送信装置31との間でのデータ通信の仲介を行う手段である。

AKE手段53は、AVコンテンツ送信装置31との間で認証・鍵交換を行う手段であって、AVコンテンツ送信装置31との間で認証が成功した場合、そのAVコンテンツ送信装置31から交換鍵K_{ex}を入力する手段である。

K_{co}要求コマンド発行手段54は、基本暗号化手法に対応する暗号化鍵K_{co}の種を送信するようにAVコンテンツ送信装置31に対して要求するコマンドを発行する手段である。また、K_{co}要求コマンド発行手段54は、その要求コマンドに対応する、AVコンテンツ送信装置31からの最新の暗号化鍵K_{co}の種を入力する手段でもある。

K_{co}記憶手段55は、あらかじめ、AVコンテンツ送信装置31からの暗号化されたAVコンテンツを解読するさいに必要となる所定の関数が設定されており、AKE手段53からの交換鍵K_{ex}を入力するとともに、K_{co}要求コマンド発行手段54からの暗号化鍵K_{co}の種を入力し、交換鍵K_{ex}と暗号化鍵K_{co}とをあらかじめ設定されている関数に代入して暗号化鍵K_{co}を生成し記憶する手段である。

暗号解読手段56は、AVコンテンツ送信装置31からの暗号化されたAVコンテンツを入力するとともに、K_{co}記憶手段55からの暗号化鍵K_{co}を入力し、基本暗号化手法に基づいて、暗号化されたAVコンテンツを暗号化鍵K_{co}で解読する手段である。なお、暗号解読手段56は、基本暗号化手法のみを使用することができるものであるとする。いいかえると、暗号解読手段56は、拡張暗号化手法を使用することができないものである。

次に、IEEE 1394バスは、AVコンテンツ送信装置31、第1のAVコンテンツ受信装置32および第2のAVコンテンツ受信装置33それぞれの間で通信されるデータの伝送路である。

また、アンテナ34は、AVコンテンツ送信装置31外部に設置され、AVコンテンツを受信する手段である。モニタ35は、第1のAVコンテンツ受信装置32からのAVコンテンツを表示する手段であり、同様に、モニタ36は、第2のAVコンテンツ受信装置33からのAVコンテンツを表示する手段である。

次に、本発明の第3の実施の形態のAVコンテンツ通信システムの動作を述べる。

図9のAVコンテンツ通信システムの動作を詳しく述べる前に、以下の説明の便宜上、次に示す状況を想定し、その状況下でのAVコンテンツ通信システムの動作を述べることにする。

その状況とは、先ず、AVコンテンツ送信装置31がアンテナ34からのAVコンテンツを拡張暗号化手法を用いて暗号化してIEEE 1394バスに出力しており、そのAVコンテンツの出力の途中から、第1のAVコンテンツ受信装置32がそのAVコンテンツを受信して解読し、さらにその後、拡張暗号化手法を使用することができない第2のAVコンテンツ受信装置33がそのAVコンテンツを受信して解読しようとする状況である。

さて、はじめに、AVコンテンツ送信装置31がアンテナ34からのAVコンテンツを拡張暗号化手法を用いて暗号化しIEEE 1394バスに出力するまでのAVコンテンツ送信装置31の動作を述べる。なお、AVコンテンツ送信装置31は、上述したように、拡張暗号化手法を使用することでも

きるし、基本暗号化手法を使用することもできるが、出力するAVコンテンツの内容をより強く保護するという目的のために、基本暗号化手法を使用して暗号化したAVコンテンツを出力するように要求されることがなければ、暗号化強度のより強い拡張暗号化手法を使用してAVコンテンツを暗号化するものとする。

まず、暗号化手法選択手段40は、拡張暗号化手法を選択し、受信手段37は、AVコンテンツ送信装置31外部のアンテナ34を介してAVコンテンツを受信し、暗号化手段38は、受信手段37からのAVコンテンツを入力するとともに、Kco生成手段39からの暗号化鍵Kco1を入力し、その後、拡張暗号化手法に基づいて、暗号化鍵Kco1でAVコンテンツを暗号化する。なお、Kco生成手段39からの暗号化鍵を、拡張暗号化手法に対応する暗号化鍵であることを示すために、「Kco1」というように記述した。また、以下では、その拡張暗号化手法とは別の基本暗号化手法に対応する暗号化鍵を「Kco2」というように記述する。ところで、暗号化は、例えばAVコンテンツの一部のヘッダについては行われないものとする。つまり、AVコンテンツが受信されたさいに、暗号化鍵Kco1がなくてもそのAVコンテンツのヘッダ情報は解読されるが、そのAVコンテンツの内容は暗号化鍵Kco1がなくては解読されないように暗号化が行われるものとする。また、暗号化手段38が利用するKco生成手段39からの暗号化鍵Kco1は、上述したように20秒毎に更新されるものとする。そして、Kco生成手段39は、暗号化鍵Kco1がどのタイミングで更新するのかという情報として、oddまたはevenを出力する。そのoddまたはevenは、互いに相手方から切り替わったときに、その切り替わりの前後でA

Vコンテンツの暗号化に使用された暗号化鍵K c o 1が20秒毎の更新により切り替わっていることを示すためのものであるとする。その後、データ転送手段44は、暗号化手段38からの暗号化鍵K c o 1で暗号化されたAVコンテンツ、つまりK c o (AVコンテンツ)を入力するとともに、K c o生成手段39からのo d dまたはe v e nを入力し、図10(a)に示すように、K c o (AVコンテンツ)のヘッダのなかにo d dまたはe v e nを付加してI E E E 1 3 9 4バスに出力する。なお、図10(a)は、AVコンテンツ送信装置31から送信されるAVコンテンツの構成図である。図10(b)については後に説明する。

次に、上述したようにしてAVコンテンツ送信装置31がAVコンテンツを暗号化してI E E E 1 3 9 4バスに出力しているときに、その途中から、第1のAVコンテンツ受信装置32がそのAVコンテンツを解読するところまでのAVコンテンツ送信装置31と第1のAVコンテンツ受信装置32の動作を述べる。

このとき、第1のAVコンテンツ受信装置32のAKE手段46は、AVコンテンツ送信装置31のAKE手段41に対して、認証要求を行い、AKE手段46およびAKE手段41は、互いに相手方の装置の認証を行う。その認証が成功すると、AKE手段41は、AKE手段46に交換鍵K e xを出力する。その交換鍵K e xは、暗号化されたAVコンテンツを解読するさいに必要となる鍵である。それとともに、AKE手段41は、第1のAVコンテンツ受信装置32が拡張暗号化手法を使用することができるものであることを判断し、暗号化手法の変更を行わない。なお、AKE手段46およびAKE手段41が行う認証が失敗した場合、AKE手段41は、AKE手段

46に交換鍵 K_{ex} を出力することはない。ここでは、以下の説明の便宜上、AKE手段46およびAKE手段41が行う認証は成功するものとする。

そして、第1のAVコンテンツ受信装置32のAKE手段46は、データ転送手段45を介して、AKE手段41からの交換鍵 K_{ex} を入力し、 K_{co} 記憶手段49に出力する。また、暗号化手法通知検出手段47は、AVコンテンツ送信装置31からのAVコンテンツが拡張暗号化手法で暗号化されたものであることを検出し、その旨の情報、つまり拡張暗号化手法を暗号化手法記憶手段50に出力し記憶させる。さらに、 K_{co} 要求コマンド発行手段48は、拡張暗号化手法に対応する最新の暗号化鍵 K_{co1} の種を送信するように、AVコンテンツ送信装置31の K_{co} 要求コマンド応答手段43に対してコマンドを発行し、そのコマンドに対応する K_{co} 要求コマンド応答手段43からの最新の暗号化鍵 K_{co1} の種を入力して、その種を K_{co} 記憶手段49に出力する。なお、上述したように、AVコンテンツ送信装置31からの暗号化鍵 K_{co1} が20秒毎に更新されるので、 K_{co} 要求コマンド発行手段48は、 K_{co} 要求コマンド応答手段43に対するコマンドを20秒毎に発行するものとする。その後、 K_{co} 記憶手段49は、後述する(数1)に示すように、あらかじめ設定されている関数に、AKE手段46からの交換鍵 K_{ex} と、 K_{co} 要求コマンド発行手段48からの暗号化鍵 K_{co1} の種とを代入し、暗号化鍵 K_{co1} を生成し記憶する。なお、(数1)の $seed$ のところに、暗号化鍵 K_{co1} の種を代入する。

【数1】

$$K_{co} = f(seed, K_{ex})$$

そして、AVコンテンツ送信装置31からの K_{co} (AVコンテンツ) のへ

ッダのなかのoddまたはevenを検出し、さらに、oddとevenとの切り替わりを判断して、AVコンテンツ送信装置31からのKco（AVコンテンツ）がどの暗号化鍵Kco1で暗号化されたのかを特定する。なお、上述したように、oddとevenとの切り替わりは、その切り替わりの前後でAVコンテンツの暗号化に使用された暗号化鍵Kco1が切り替わっていることを示す。また、AVコンテンツ送信装置31のKco要求コマンド応答手段43は、Kco要求コマンド発行手段48からの、暗号化鍵Kco1の種の送信要求のコマンドを入力すると、そのコマンドにしたがって、暗号化鍵Kco1の種をデータ転送手段44に出力する。そして、データ転送手段44は、図10（b）に示すように、Kco（AVコンテンツ）に使用した暗号化鍵Kco1の種を、Kco（AVコンテンツ）とは別の非同期信号を使用してコマンドでIEEE1394バスに出力する。なお、図10（b）は、AVコンテンツ送信装置31から送信されるコマンドの構成図である。

最後に、暗号解読手段51は、AVコンテンツ送信装置31からの暗号化されたAVコンテンツをデータ転送手段45を介して入力するとともに、Kco記憶手段49からの暗号化鍵Kco1と、暗号化手法記憶手段50からの拡張暗号化手法とを入力し、その拡張暗号化手法に基づいて、暗号化されたAVコンテンツを暗号化鍵Kco1で解読し、モニタ35に出力する。そして、モニタ35は、暗号解読手段51からのAVコンテンツの内容を表示する。

次に、上述したようにして、AVコンテンツ送信装置31が拡張暗号化手法を使用してAVコンテンツを暗号化して出力し、第1のAVコンテンツ受

信装置 3 2 がその AV コンテンツを解読しているときに、拡張暗号化手法を使用することができない第 2 の AV コンテンツ受信装置 3 3 がその AV コンテンツを解読するさいの AV コンテンツ送信装置 3 1、第 1 の AV コンテンツ受信装置 3 2 および第 2 の AV コンテンツ受信装置 3 3 の動作を述べる。なお、そのさいの AV コンテンツ送信装置 3 1 の動作については図 1 1 のフローチャートをも用いて説明する。

さて、第 2 の AV コンテンツ受信装置 3 3 の AKE 手段 5 3 は、AV コンテンツ送信装置 3 1 の AKE 手段 4 1 に対して、認証要求を行い、AKE 手段 5 3 および AKE 手段 4 1 は、互いに相手方の装置の認証を行う（図 1 1 のステップ 1）。そのさい、AKE 手段 5 3 は、AV コンテンツ送信装置 3 1 が出力する AV コンテンツの暗号化手法を、基本暗号化手法にするように要求する。なぜなら、第 2 の AV コンテンツ受信装置 3 3 は、拡張暗号化手法を使用することができず、基本暗号化手法しか使用することができないからである。そして、互いの認証が成功すると、AKE 手段 4 1 は、その要求を受け入れ（図 1 1 のステップ 2）、暗号化手法選択手段 4 0 および暗号化手法変更通知手段 4 2 に、暗号化手法を基本暗号化手法にするように制御するための情報を出力する（図 1 1 のステップ 3）。その後、AKE 手段 4 1 は、AKE 手段 5 3 に交換鍵 K_{ex} を出力し、AKE 手段 4 1 と AKE 手段 5 3 との間の認証・鍵交換は完了する（図 1 1 のステップ 4）。なお、交換鍵 K_{ex} は、暗号化された AV コンテンツを解読するさいに必要となる鍵である。また、AKE 手段 5 3 および AKE 手段 4 1 が行う認証が失敗した場合、AKE 手段 4 1 は、AKE 手段 5 3 に交換鍵 K_{ex} を出力することもないし、暗号化手法を基本暗号化手法にするようにとの要求を受け入れること

もない。ただしここでは、以下の説明の便宜上、AKE手段53およびAKE手段41が行う認証は成功するものとする。

そして、AVコンテンツ送信装置31では、暗号化手法選択手段40が、AKE手段41からの、暗号化手法を基本暗号化手法にするための情報、つまり暗号化手法を変更させるための情報にしたがって、基本暗号化手法を選択し、その旨の情報を、暗号化手段38とKco生成手段39とに出力する。なお、暗号化手法選択手段40は、AKE手段41とAKE手段53との間の認証・鍵交換が完了するまでに、いいかえると、AKE手段53が交換鍵Kexを入力するまでに、基本暗号化手法を選択する。その後、Kco生成手段39は、その暗号化手法の基本暗号化手法への変更の情報を入力した後であって、かつ、拡張暗号化手法にしたがって生成していた暗号化鍵Kco1の次の更新タイミングから、基本暗号化手法にしたがった暗号化鍵Kco2を生成し、20秒毎に更新してゆく。また、暗号化手法変更通知手段42は、AVコンテンツの暗号化手法を拡張暗号化手法から基本暗号化手法に変更するという旨の情報のコマンドを、第1のAVコンテンツ受信装置32の暗号化手法通知検出手段47に出力するとともに、その暗号化手法の切り替えのタイミングの情報のコマンドを暗号化手法通知検出手段47に出力する。

その後、AVコンテンツ送信装置31の暗号化手段38は、受信手段37からのAVコンテンツを入力するとともに、Kco生成手段39からの暗号化鍵Kco2を入力し、基本暗号化手法に基づいて、暗号化鍵Kco2でAVコンテンツを暗号化する。さらに、Kco生成手段39は、暗号化鍵Kco2がどのタイミングで切り替わるのかという情報としてoddまたはevenを出力する。そして、データ転送手段44は、暗号化手段38からの暗

号化鍵K c o 2で暗号化されたAVコンテンツ、つまりK c o (AVコンテンツ)を入力するとともに、K c o生成手段39からのo d dまたはe v e nを入力し、K c o (AVコンテンツ)のヘッダのなかにo d dまたはe v e nを付加してI E E E 1 3 9 4バスに出力する。

このようにAVコンテンツ送信装置31からのAVコンテンツの暗号化手法が基本暗号化手法に切り替わると、第2のAVコンテンツ受信装置33は、そのAVコンテンツを解読することができるようになる。そこで次に、このときの第2のAVコンテンツ受信装置33がAVコンテンツを解読するさいの動作を述べる。

まず、AKE手段53は、AVコンテンツ送信装置31のAKE手段41からの交換鍵K e xを、データ転送手段52を介して入力し、K c o記憶手段55に出力する。また、K c o要求コマンド発行手段54は、基本暗号化手法に対応する暗号化鍵K c o 2の種を送信するように、AVコンテンツ送信装置31のK c o要求コマンド応答手段43に対してコマンドを発行し、そのコマンドに対応する、K c o要求コマンド応答手段43からの暗号化鍵K c o 2の種を入力して、その種をK c o記憶手段55に出力する。その後、K c o記憶手段55は、(数1)を用いて上述したようにして、あらかじめ設定されている関数に、AKE手段53からの交換鍵K e xと、K c o要求コマンド発行手段54からの暗号化鍵K c o 2の種とを代入し、暗号化鍵K c o 2を生成し記憶する。そして、AVコンテンツ送信装置31からのK c o (AVコンテンツ)のヘッダのなかのo d dまたはe v e nを検出し、さらに、o d dとe v e nとの切り替わりを判断して、AVコンテンツ送信装置31からのK c o (AVコンテンツ)がどの暗号化鍵K c o 2で暗号化

されたのかを特定する。

最後に、暗号解読手段56は、AVコンテンツ送信装置31からの暗号化されたAVコンテンツをデータ転送手段52を介して入力するとともに、Kco記憶手段55からの暗号化鍵Kco2を入力し、基本暗号化手法に基づいて、暗号化されたAVコンテンツを暗号化鍵Kco2で解読し、モニタ36に出力する。そして、モニタ36は、暗号解読手段56からのAVコンテンツの内容を表示する。

このように、AVコンテンツ送信装置31がAVコンテンツの暗号化手法を基本暗号化手法に変更してAVコンテンツを暗号化し出力すると、第2のAVコンテンツ受信装置33は、そのAVコンテンツを解読することができるようになるが、それまで拡張暗号化手法によって暗号化されたAVコンテンツを受信し解読していた第1のAVコンテンツ受信装置32は、そのままでは、そのAVコンテンツを解読することができなくなる。そこで次に、AVコンテンツ送信装置31がAVコンテンツの暗号化手法を基本暗号化手法に変更した場合、第1のAVコンテンツ受信装置32がそのAVコンテンツを解読するさいの、第1のAVコンテンツ受信装置32の動作を述べる。なお、そのさいの第1のAVコンテンツ受信装置32の動作については図12のフローチャートをも用いて説明する。

さてそのとき、上述したように、第1のAVコンテンツ受信装置32の暗号化手法通知検出手段47は、AVコンテンツ送信装置31の暗号化手法変更通知手段42からの、AVコンテンツの暗号化手法が拡張暗号化手法から基本暗号化手法に変更するという旨の情報のコマンドを入力するとともに、その暗号化手法の切り替えのタイミングの情報のコマンドも入力する（図1

2のステップ1)。そして、暗号化手法通知検出手段47は、それら2つの情報を、Kco要求コマンド発行手段48と暗号化手法記憶手段50とに出力する。その後、Kco要求コマンド発行手段48は、基本暗号化手法に対応する暗号化鍵Kco2の種を送信するように、AVコンテンツ送信装置31のKco要求コマンド応答手段43に対してコマンドを発行し(図12のステップ2)、そのコマンドに対応する、Kco要求コマンド応答手段43からの暗号化鍵Kco2の種を入力して、その種をKco記憶手段49に出力する。その後、Kco記憶手段49は、あらかじめ設定されている関数に、AKE手段46からの交換鍵Kexと、Kco要求コマンド発行手段48からの暗号化鍵Kco2の種とを代入し、暗号化鍵Kco2を生成し記憶する(図12のステップ3)。

最後に、暗号解読手段51は、AVコンテンツ送信装置31からの暗号化されたAVコンテンツをデータ転送手段45を介して入力するとともに、Kco記憶手段49からの暗号化鍵Kco2と、暗号化手法記憶手段50からの基本暗号化手法とを入力する。そして、暗号解読手段51は、基本暗号化手法を使用することができるので、その基本暗号化手法に基づいて、暗号化されたAVコンテンツを暗号化鍵Kco2で解読し、モニタ35に出力する(図12のステップ4)。そして、モニタ35は、暗号解読手段51からのAVコンテンツの内容を表示する。

このように、AVコンテンツ送信装置31がAVコンテンツの暗号化手法を基本暗号化手法に変更した場合であっても、第1のAVコンテンツ受信装置32は、暗号化手法が基本暗号化手法に切り替わったという情報と、その切り替えのタイミングの情報とを入力することによって、基本暗号化手法に

よって暗号化されたAVコンテンツを解読することができるようになる。

ところで、AVコンテンツ送信装置31がAVコンテンツの暗号化手法を基本暗号化手法に変更してAVコンテンツを送信しているとき、第2のAVコンテンツ受信装置33がそのAVコンテンツを解読することを中止することがある。以下に、そのような第2のAVコンテンツ受信装置33がAVコンテンツを解読することを中止する場合のAVコンテンツ送信装置31および第1のAVコンテンツ受信装置32の動作を述べる。

さて、第2のAVコンテンツ受信装置33がAVコンテンツを解読することを中止する場合、第2のAVコンテンツ受信装置33のKco要求コマンド発行手段54は、暗号化鍵Kco2の種を送信するように、AVコンテンツ送信装置31のKco要求コマンド応答手段43に対してコマンドを発行しなくなる。つまり、Kco要求コマンド応答手段43にとっては、Kco要求コマンド発行手段54からのコマンドを受信しなくなるということである。このように、Kco要求コマンド応答手段43は、Kco要求コマンド発行手段54からのコマンドを受信しなくなると、第2のAVコンテンツ受信装置33がAVコンテンツを解読することを中止したものと判断する。そして、Kco要求コマンド応答手段43は、第2のAVコンテンツ受信装置33がAVコンテンツを解読することを中止したことを、暗号化手法変更通知手段42に通知する。

その後、暗号化手法変更通知手段42は、Kco要求コマンド応答手段43からの、第2のAVコンテンツ受信装置33がAVコンテンツを解読することを中止したとする情報を入力し、その情報に基づいて、暗号化手法選択手段40に対して、選択する暗号化手法を基本暗号化手法から拡張暗号化手

法に切り替えさせるとともに、第1のAVコンテンツ受信装置32の暗号化手法通知検出手段47に対して、暗号化手法が基本暗号化手法から拡張暗号化手法に切り替わるという情報を、その切り替えのタイミングの情報とともに出力する。このように、暗号化手法を拡張暗号化手法に切り替えるのは、上述したように拡張暗号化手法の方が基本暗号化手法よりも暗号化の強度が強く、不正な装置にAVコンテンツの内容を解読させないようにする防御をより強くするためである。なお、暗号化手法を基本暗号化手法から拡張暗号化手法に切り替えるさい、あらかじめAKE手段41に、第2のAVコンテンツ受信装置33が基本暗号化手法しか使用することができないということを記憶させておき、その後、暗号化手法変更通知手段42に、第2のAVコンテンツ受信装置33がAVコンテンツを解読することを中止した場合、暗号化手法を基本暗号化手法から拡張暗号化手法に切り替えるように判断できればよい。

そして、暗号化手法選択手段40は、暗号化手法の選択を基本暗号化手法から拡張暗号化手法に再度切り替える。このように暗号化手法が拡張暗号化手法に切り替えられた後のAVコンテンツ送信装置31の各構成手段は、上述した基本暗号化手法に切り替えられる前の拡張暗号化手法に基づいてAVコンテンツを暗号化し出力していたときと同じ動作を行う。

他方、第1のAVコンテンツ受信装置32では、暗号化手法通知検出手段47が、AVコンテンツ送信装置31の暗号化手法変更通知手段42からの、暗号化手法が基本暗号化手法から拡張暗号化手法に切り替わるという情報と、その切り替えのタイミングの情報とを入力する。そして、その情報にしたがって、暗号解読するさいの各構成手段が動作を切り替える。その切り替

わりのタイミングは、暗号化手法が拡張暗号化手法から基本暗号化手法に切り替わったタイミングと同様であって、またその切り替え後の第1のAVコンテンツ受信装置32の各構成手段は、上述した基本暗号化手法に切り替えられる前の拡張暗号化手法に基づいて暗号化されたAVコンテンツを解読するさいの動作と同じように動作する。

このように、AVコンテンツ送信装置31がAVコンテンツの暗号化手法を基本暗号化手法を使用して暗号化しAVコンテンツを送信しているとき、第2のAVコンテンツ受信装置33がそのAVコンテンツを解読することを中止した場合、AVコンテンツ送信装置31は、暗号化強度のより強い拡張暗号化手法で暗号化したAVコンテンツを送信するように変更する。このように暗号化手法が基本暗号化手法から拡張暗号化手法に変更された場合であっても、第1のAVコンテンツ受信装置32は、それに対応してそのAVコンテンツを解読することができる。

なお、上述した第3の実施の形態では、AVコンテンツ送信装置31の暗号化手法変更通知手段42は、AVコンテンツの暗号化手法が拡張暗号化手法から基本暗号化手法に変更するという旨の情報のコマンドを第1のAVコンテンツ受信装置32の暗号化手法通知検出手段47に出力するとした。しかしながら、暗号化手法変更通知手段42は、AVコンテンツの暗号化手法が拡張暗号化手法から他の暗号化手法に変更するという旨の情報を暗号化手法通知検出手段47に出力するとしてもよい。ただしこの場合、暗号化手法通知検出手段47は、変更後の暗号化手法がどのような暗号化手法であるのかを通知するように、AVコンテンツ送信装置31に要求しなければならない。同様に、暗号化手法変更通知手段42は、暗号化手法の拡張暗号化手法

から基本暗号化手法への切り替えのタイミングの情報をコマンドで暗号化手法通知検出手段 4 7 に出力するとしたが、暗号化手法変更通知手段 4 2 は、そのような暗号化手法の切り替えのタイミングの情報を暗号化手法通知検出手段 4 7 に出力しないとしてもよい。ただしこの場合も、暗号化手法通知検出手段 4 7 は、暗号化手法の切り替えのタイミングの情報を通知するように、AV コンテンツ送信装置 3 1 に要求しなければならない。また、暗号化手法変更通知手段 4 2 が出力する暗号化手法の切り替えの情報や切り替えのタイミングの情報は、コマンドではなく、AV コンテンツのなかに付加されたものであってもよい。

また、上述した第 3 の実施の形態では、AV コンテンツ送信装置 3 1 は、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるさい、暗号化手法のみがどのような暗号化手法に切り替わるのかという情報を出力し、その後、第 1 の AV コンテンツ受信装置 3 2 から、その変更後の暗号化手法に対応する暗号化鍵 K c o の種を送信するように要求された場合、その要求にしたがって、暗号化鍵 K c o の種を送信するとした。しかしながら、AV コンテンツ送信装置 3 1 は、暗号化手法を切り替えるさい、切り替わった後の暗号化手法の情報とともに、その変更後の暗号化手法に対応する暗号化鍵 K c o の種を出力するとしてもよい。また、AV コンテンツ送信装置 3 1 は、暗号化鍵 K c o の種を出力するとしたが、暗号化鍵 K c o そのもの、または交換鍵 K e x で暗号化した暗号化鍵 K c o を出力してもよい。その場合、受信側では、種ではなく、暗号化鍵 K c o そのもの、または交換鍵 K e x で暗号化された暗号化鍵 K c o が使用されることになる。また、暗号化鍵 K c o の種はコマンドを利用して送信されるとしたが、暗号化鍵 K c o やその種は

、コマンドで送信されても、AVコンテンツのなかに付加されて送信されてもよい。

また、上述した第3の実施の形態では、AVコンテンツ送信装置31のKco生成手段39は、20秒毎に暗号化鍵Kcoを更新するとしたが、Kco生成手段39が暗号化鍵Kcoを更新する間隔は、20秒毎という間隔に限定されるものではない。暗号化鍵Kcoは、定期的に更新されてもよいし、不定期に更新されてもよい。

また、上述した第3の実施の形態では、AVコンテンツ送信装置31が第2のAVコンテンツ受信装置33を記憶し、その第2のAVコンテンツ受信装置33から、AVコンテンツを解読するための暗号化鍵Kco2の種を要求するコマンドが来ているか否かを判断し、そのコマンドが来なくなった場合、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるとした。しかしながら、AVコンテンツ送信装置31が、第1のAVコンテンツ受信装置32と第2のAVコンテンツ受信装置33とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということ調べておき、AVコンテンツを解読するための暗号化鍵Kcoの種を要求するコマンドを送信してくるAVコンテンツ受信装置が、全て拡張暗号化手法を使用することができるAVコンテンツ受信装置である場合、暗号化手法を基本暗号化手法から拡張暗号化手法に切り替えるとしてもよい。

また、上述した第3の実施の形態では、AVコンテンツ送信装置31が暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるさい、まず、AVコンテンツ送信装置31は、第2のAVコンテンツ受信装置33との間で互いに認証を行い、その認証が成功すると、暗号化手法を拡張暗号化手法か

ら基本暗号化手法に切り替えるとした。しかしながら、図13に示すように、AVコンテンツ送信装置31は、第2のAVコンテンツ受信装置33からの認証要求を受信した後（図13のステップ1）、互いの認証が成功するかどうかにかかわらず、暗号化手法を拡張暗号化手法から基本暗号化手法へ変更し（図13のステップ2）、その変更の後、認証が成功すると（図13のステップ3）、暗号化手法を基本暗号化手法に決定するとしてもよい（図13のステップ5）。なお、図13のステップ3で認証が失敗すると、暗号化手法を基本暗号化手法から拡張暗号化手法に再変更して暗号化手法を決定するとしてもよい（図13のステップ4）。

また、上述した第3の実施の形態では、AVコンテンツ送信装置31は、第2のAVコンテンツ受信装置33との間で互いに認証を行い、その認証が成功した場合に、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるとした。しかしながら、AVコンテンツ送信装置31は、第2のAVコンテンツ受信装置33からの認証要求を受信すると、認証が成功するか失敗するかにかかわらず、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えて、その切り替えた後の基本暗号化手法でAVコンテンツを暗号化して出力してもよい。ただしこの場合、AVコンテンツ送信装置31と第2のAVコンテンツ受信装置33との間での認証が失敗すると、AVコンテンツ送信装置31は、第2のAVコンテンツ受信装置33に交換鍵 K_{ex} を出力しない。したがって、AVコンテンツ送信装置31からのAVコンテンツは、不正な装置に解読されないように保護される。他方、AVコンテンツ送信装置31が第2のAVコンテンツ受信装置33からの認証要求を受信して、暗号化手法を基本暗号化手法に切り替えて暗号化したAVコンテンツを出力

する場合、上述した第3の実施の形態で説明したとおり、第1のAVコンテンツ受信装置32は、AVコンテンツ送信装置31からの、暗号化手法が基本暗号化手法に切り替わるという情報を入力し、AVコンテンツ送信装置31からの基本暗号化手法で暗号化されたAVコンテンツを入力して、基本暗号化手法でそのAVコンテンツを解読することになる。一方その後、AVコンテンツ送信装置31は、第2のAVコンテンツ受信装置33が不正であると判断した時点で、拡張暗号化手法に再変更する。

また、上述した第3の実施の形態のAVコンテンツ通信システムの各構成手段・構成要素の全部または一部は、ハードウェアであつてもよいし、そのハードウェアの該当する機能と同じ機能を有するソフトウェアであつてもよい。

さらに、請求項25の本発明は、請求項16から24のいずれかに記載のAVコンテンツ送信方法の各ステップの全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体である。また、請求項28の本発明は、請求項26または27記載のAVコンテンツ受信方法の各ステップの全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体である。

産業上の利用可能性

以上説明したところから明らかなように、請求項1の本発明は、コントロールキー更新によりセキュリティを高め、認証・鍵交換の実行回数を減らすことによって送受信効率を高めるデータ送受信方法を提供することができる。

また、請求項6の本発明は、コントロールキー更新によりセキュリティを高め、認証・鍵交換の実行回数を減らすことによって送受信効率を高めるデータ送信装置を提供することができる。また、請求項8の本発明は、コントロールキー更新によりセキュリティを高め、認証・鍵交換の実行回数を減らすことによって送受信効率を高めるデータ受信装置を提供することができる。さらに、請求項14の本発明は、コントロールキー更新によりセキュリティを高め、認証・鍵交換の実行回数を減らすことによって送受信効率を高めるデータ送受信システムを提供することができる。また、請求項15の本発明は、本発明の各装置に備えられた各構成手段の全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したプログラム記録媒体を提供することができる。

また、本発明は、AVコンテンツ送信装置が第1の暗号化手法で暗号化したAVコンテンツを送信しているときに、その第1の暗号化手法を使用することができないAVコンテンツ受信装置がそのAVコンテンツを解読することができるようにするAVコンテンツ送信方法を提供することができる。

また、本発明は、第1の暗号化手法で暗号化したAVコンテンツを送信しているときに、その第1の暗号化手法を使用することができないAVコンテンツ受信装置がそのAVコンテンツを解読することができるようにするAVコンテンツ送信装置を提供することができる。

また、本発明は、上述したAVコンテンツ送信方法を用いたさい、第1の暗号化手法で暗号化されたAVコンテンツを受信し解読していた、第1の暗号化手法を使用することができないAVコンテンツ受信装置とは別のAVコンテンツ受信装置がある場合、その別のAVコンテンツ受信装置が引き続き

そのAVコンテンツを解読することができるようにするAVコンテンツ送信方法およびAVコンテンツ受信方法を提供することができる。

さらに、本発明は、上述したAVコンテンツ送信装置が第1の暗号化手法を使用することができないAVコンテンツ受信装置にそのAVコンテンツを解読させる場合、そのAVコンテンツ受信装置とは別に、第1の暗号化手法で暗号化されていたAVコンテンツを引き続き解読するAVコンテンツ受信装置を提供することができる。

請 求 の 範 囲

1. 送信側が、デジタルデータにワークキーを用いて第1の暗号化を施した暗号化デジタルデータと、前記ワークキーにコントロールキーを用いて第2の暗号化を施した暗号化ワークキーとを送信し、受信側が、前記送信側と認証・鍵交換を行うことによって得た前記コントロールキーを用いて、受信した前記暗号化ワークキーを解読し、解読して得られた前記ワークキーを用いて受信した前記暗号化デジタルデータを解読して、前記デジタルデータを得るデータ送受信方法において、前記送信側は、前記コントロールキーを定期的または不定期的に更新するとともに、前記コントロールキー毎に前記コントロールキーを特定できる識別子を付与し、前記受信側は、受信中断後に受信を再開する際に、前記送信側から送信されてきた前記識別子を参照することにより、前記受信中断中に前記コントロールキーが更新されたか否かを判断し、前記コントロールキーが更新されたと判断した場合には、前記認証・鍵交換を改めて行うことによって、更新後の前記コントロールキーを得ることを特徴とするデータ送受信方法。

2. 前記受信側は、前記送信側に対して、受信中断後に受信を再開する際に、前記識別子の送信を要求し、前記送信側は、前記認証・鍵交換を行う際に前記識別子を送信するのに加えて、前記要求に応じて前記識別子を送信することを特徴とする請求項1記載のデータ送受信方法。

3. 前記送信側は、定期的または不定期的に、前記識別子を前記受信側へ送信することを特徴とする請求項1記載のデータ送受信方法。

4. 前記送信側は、前記ワークキーを定期的または不定期的に更新し、前記ワークキーに前記第1の暗号化を施す際に用いた前記コントロールキー

に対応する前記識別子を、前記ワークキーとともに前記受信側へ送信することを特徴とする請求項 3 記載のデータ送受信方法。

5. 前記送信側は、前記コントロールキーの更新を行った後、更新された前記コントロールキーに対しての前記認証・鍵交換が完了するまでの間は、前記ワークキーの更新を行わないことを特徴とする請求項 1 から 4 のいずれかに記載のデータ送受信方法。

6. ワークキーを定期的または不定期的に更新生成し、デジタルデータに前記ワークキーを用いて第 1 の暗号化を施して暗号化デジタルデータに変換して、データ受信装置へ送信する暗号化手段と、

コントロールキーを定期的または不定期的に更新生成し、前記ワークキーに前記コントロールキーを用いて第 2 の暗号化を施して暗号化ワークキーに変換して、前記データ受信装置へ送信する鍵暗号化手段と、

前記データ受信装置との認証・鍵交換を行う送信側認証・鍵交換手段と、
前記コントロールキーを特定できる識別子を生成する識別子生成手段と、
前記識別子を前記データ受信装置へ送信する識別子送信手段とを
備えたことを特徴とするデータ送信装置。

7. 前記暗号化手段は、前記鍵暗号化手段が前記コントロールキーの更新を行った後、前記更新されたコントロールキーに対しての前記認証・鍵交換が完了するまでの間は、前記ワークキーの更新を行わないことを特徴とする請求項 6 記載のデータ送信装置。

8. データ送信装置との認証・鍵交換を行う受信側認証・鍵交換手段と

ワークキーにコントロールキーを用いて第 2 の暗号化を施して変換された

暗号化ワークキーを、前記受信側認証・鍵交換手段を介して得られた前記コントロールキーを用いて解読して、前記ワークキーを復元する鍵復元手段と

、
デジタルデータに前記ワークキーを用いて第1の暗号化を施して変換された暗号化デジタルデータを、前記鍵復元手段によって復元された前記ワークキーを用いて解読して、前記デジタルデータを復元する暗号解読手段と、

少なくとも、受信中断後に受信を再開する際に、前記データ送信装置から送信されてきた、前記コントロールキーを特定するための識別子を参照することにより、前記コントロールキーが更新されたか否かを判断し、前記コントロールキーが更新されたと判断した場合には、前記受信側認証・鍵交換手段に前記認証・鍵交換を改めて行って更新後の前記コントロールキーを得ることを指示する識別子認識手段とを

備えたことを特徴とするデータ受信装置。

9. 前記識別子を記憶する識別子記憶手段を備え、前記識別子認識手段は、前記データ送信装置から送信されてきた最新の前記識別子を、前記識別子記憶手段に記憶されている、その直前に送信されてきた前記識別子と比較することによって、前記コントロールキーが更新されたか否かを判断することを特徴とする請求項8記載のデータ受信装置。

10. 前記識別子送信手段は、前記認証・鍵交換が行われる際に前記識別子を送信するのに加えて、前記データ受信装置からの要求に応じて、前記識別子を送信することを特徴とする請求項6または7記載のデータ送信装置。

11. 前記受信中断後に受信を再開する際に、前記識別子を送信することを前記データ送信装置に対して要求する識別子要求手段を備えることを特徴とする請求項8または9記載のデータ受信装置。

12. 前記識別子送信手段は、定期的または不定期的に、前記識別子を前記データ受信装置へ送信することを特徴とする請求項6または7記載のデータ送信装置。

13. 前記識別子送信手段は、前記ワークキーが更新生成される度に、前記更新生成されたワークキーに前記第2の暗号化を施す際に用いた前記コントロールキーに対応する前記識別子を、前記データ受信装置へ送信することを特徴とする請求項12記載のデータ送信装置。

14. 請求項6、7、12、13のいずれかに記載のデータ送信装置および請求項8または9記載のデータ受信装置、または、請求項10記載のデータ送信装置および請求項11記載のデータ受信装置を備えたことを特徴とするデータ送受信システム。

15. 請求項6から13のいずれかに記載のデータ送信装置またはデータ受信装置の各構成手段の全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体。

16. AVコンテンツ送信装置が伝送路を利用して第1の暗号化手法で暗号化したAVコンテンツを送信しているときに、

その第1の暗号化手法を使用することができないAVコンテンツ受信装置から認証要求があると、

その認証要求をしたAVコンテンツ受信装置が使用することができる第2の暗号化手法で前記AVコンテンツを暗号化して送信する

ことを特徴とするAVコンテンツ送信方法。

17. 前記認証要求があったさい、既にそれまでの前記第1の暗号化手法で暗号化されたAVコンテンツを受信し解読していた、前記認証要求をしたAVコンテンツ受信装置とは別のAVコンテンツ受信装置がある場合、

その別のAVコンテンツ受信装置に、暗号化手法が前記第2の暗号化手法に切り替わることを通知する

ことを特徴とする請求項16記載のAVコンテンツ送信方法。

18. 前記暗号化手法の切り替えを、所定のコマンドを用いて、または前記AVコンテンツのなかに付加して通知することを特徴とする請求項17記載のAVコンテンツ送信方法。

19. 前記切り替えた後の前記第2の暗号化手法がどのような暗号化手法であるのかという情報を、所定のコマンドを用いて、または前記AVコンテンツのなかに付加して通知することを特徴とする請求項18記載のAVコンテンツ送信方法。

20. 前記切り替えた後の前記第2の暗号化手法で使用する暗号化鍵またはその暗号化鍵の種を、所定のコマンドを用いて、または前記AVコンテンツのなかに付加して通知することを特徴とする請求項18記載のAVコンテンツ送信方法。

21. 前記暗号化手法の切り替えのタイミングを、前記認証要求がある前に使用していた前記第1の暗号化手法での暗号化鍵の更新のタイミングとすることを特徴とする請求項16記載のAVコンテンツ送信方法。

22. 少なくとも前記別のAVコンテンツ受信装置に、前記暗号化手法が前記第2の暗号化手法に切り替わることを通知するとともに、その暗号化

手法の切り替えのタイミングの情報を送信することを特徴とする請求項 17 記載の AV コンテンツ送信方法。

23. 前記 AV コンテンツ送信装置が前記認証要求をした AV コンテンツ受信装置を記憶し、

その AV コンテンツ受信装置から、前記 AV コンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドが来ているか否かを判断し、前記コマンドが来なくなった場合、

前記暗号化手法を前記第 2 の暗号化手法から前記第 1 の暗号化手法に切り替える

ことを特徴とする請求項 16 記載の AV コンテンツ送信方法。

24. 前記 AV コンテンツ送信装置が、前記認証要求をした AV コンテンツ受信装置と前記その AV コンテンツ受信装置とは別の AV コンテンツ受信装置とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、

前記 AV コンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドを送信してくる AV コンテンツ受信装置が、全て前記第 1 の暗号化手法を使用することができる AV コンテンツ受信装置である場合、

前記暗号化手法を前記第 2 の暗号化手法から前記第 1 の暗号化手法に切り替える

ことを特徴とする請求項 16 記載の AV コンテンツ送信方法。

25. 請求項 16 から 24 のいずれかに記載の AV コンテンツ送信方法の各ステップの全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体。

26. 請求項16から24のいずれかに記載のAVコンテンツ送信方法によって送信されてくるAVコンテンツを受信し、

そのAVコンテンツが暗号化されたさいに使用された暗号化手法に基づくとともに、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種を利用して、前記暗号化されたAVコンテンツを解読する

ことを特徴とするAVコンテンツ受信方法。

27. 請求項16から24のいずれかに記載のAVコンテンツ送信方法によって送信されてくるAVコンテンツとともに、またはそのAVコンテンツのなかに、前記暗号化手法の切り替えに関する情報があって、

その情報に、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種との一方または両方が含まれていない場合、

前記AVコンテンツ送信装置に対して、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種とのうちの前記暗号化手法の切り替えに関する情報に含まれていないものを送信するように要求する

ことを特徴とする請求項26記載のAVコンテンツ受信方法。

28. 請求項26または27記載のAVコンテンツ受信方法の各ステップの全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体。

29. 送信しようとするAVコンテンツを暗号化するさいの暗号化手法を選択する暗号化手法選択手段と、

その暗号化手法選択手段によって選択された暗号化手法に対応した、AV

コンテンツを暗号化するための暗号化鍵を生成する暗号化鍵生成手段と、

AVコンテンツを入力するとともに、前記暗号化鍵生成手段からの前記暗号化鍵を入力し、その暗号化鍵を利用して、前記AVコンテンツを暗号化する暗号化手段と、

AVコンテンツ受信装置との間で認証・鍵交換を行う送信側認証・鍵交換手段とを備え、

AVコンテンツ送信装置が、前記暗号化手法選択手段によって選択された第1の暗号化手法で暗号化したAVコンテンツを送信しているときに、

その第1の暗号化手法を使用することができないAVコンテンツ受信装置から認証要求があると、前記送信側認証・鍵交換手段は、その認証要求をしたAVコンテンツ受信装置との間で認証を行い、

前記暗号化手法選択手段は、暗号化手法を、前記認証要求をしたAVコンテンツ受信装置が使用することができる第2の暗号化手法に切り替える

ことを特徴とするAVコンテンツ送信装置。

30. 前記認証要求があったさい、既にそれまでの前記第1の暗号化手法で暗号化されたAVコンテンツを受信し解読していた、前記認証要求をしたAVコンテンツ受信装置とは別のAVコンテンツ受信装置がある場合、

その別のAVコンテンツ受信装置に、暗号化手法が前記第2の暗号化手法に切り替わることを通知する暗号化手法通知手段を備えた

ことを特徴とする請求項29記載のAVコンテンツ送信装置。

31. 前記暗号化鍵生成手段は、定期的または不定期に前記暗号化鍵を更新し、

前記暗号化手法選択手段が暗号化手法を前記第2の暗号化手法に切り替え

るタイミングは、前記暗号化鍵生成手段が前記第 1 の暗号化手法において暗号化鍵を更新するタイミングである

ことを特徴とする請求項 29 記載の AV コンテンツ送信装置。

32. 前記送信側認証・鍵交換手段は、前記認証要求をした AV コンテンツ受信装置を記憶するとともに、その AV コンテンツ受信装置から、前記 AV コンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドが来ているか否かを判断し、前記コマンドが来なくなったと判断した場合、

前記暗号化手法選択手段は、前記暗号化手法を前記第 2 の暗号化手法から前記第 1 の暗号化手法に切り替える

ことを特徴とする請求項 29 記載の AV コンテンツ送信装置。

33. 前記送信側認証・鍵交換手段は、前記認証要求をした AV コンテンツ受信装置と前記その AV コンテンツ受信装置とは別の AV コンテンツ受信装置とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、

前記 AV コンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドを送信してくる AV コンテンツ受信装置が、全て前記第 1 の暗号化手法を使用することができる AV コンテンツ受信装置である場合、

前記暗号化手法選択手段は、前記暗号化手法を前記第 2 の暗号化手法から前記第 1 の暗号化手法に切り替える

ことを特徴とする請求項 29 記載の AV コンテンツ送信装置。

34. 請求項 29 から 33 のいずれかに記載の AV コンテンツ送信装置との間で認証・鍵交換を行う受信側認証・鍵交換手段と、

前記ＡＶコンテンツ送信装置からの暗号化されたＡＶコンテンツのその暗号化に利用された暗号化手法の情報を入力し、記憶する暗号化手法記憶手段と、

前記ＡＶコンテンツ送信装置からの暗号化されたＡＶコンテンツを入力するとともに、前記ＡＶコンテンツ送信装置からの暗号化鍵またはその暗号化鍵の種を入力し、その後、前記暗号化手法記憶手段に記憶されている暗号化手法に基づき、かつ、前記暗号化鍵またはその暗号化鍵の種を利用して、前記暗号化されたＡＶコンテンツを解読する暗号解読手段とを備えた

ことを特徴とするＡＶコンテンツ受信装置。

３５． 請求項２９から３３のいずれかに記載のＡＶコンテンツ送信装置から送信されてくるＡＶコンテンツとともに、またはそのＡＶコンテンツのなかに、前記暗号化手法の切り替えに関する情報があって、

その情報に、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種との一方または両方が含まれていない場合、

前記ＡＶコンテンツ送信装置に対して、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種とのうちの前記情報に含まれていないものを送信するように要求する要求手段を備えた

ことを特徴とする請求項３４記載のＡＶコンテンツ受信装置。

補正書の請求の範囲

[1999年9月20日(20.09.99)国際事務局受理:新しい請求の範囲36, 37及び38が加えられた。(2頁)]

36. (追加された) 送信側は、デジタルデータにワークキーを用いて暗号化を施した暗号化デジタルデータを送信し、受信側は、前記送信側と認証・鍵交換を行うことによって、前記ワークキーを得るために必要なコントロールキーを得、前記コントロールキーを用いて得られた前記ワークキーを用いて、受信した前記暗号化デジタルデータを解読し、前記デジタルデータを得るデータ送受信方法において、

前記送信側は、前記コントロールキーを定期的または不定期的に更新するとともに、前記コントロールキー毎に前記コントロールキーを特定できる識別子を付与し、前記受信側は、受信中断後に受信を再開する際に、前記送信側から送信されてきた前記識別子を参照することにより、前記受信中断中に前記コントロールキーが更新されたか否かを判断し、前記コントロールキーが更新されたと判断した場合には、前記認証・鍵交換を改めて行うことによって、更新後の前記コントロールキーを得ることを特徴とするデータ送受信方法。

37. (追加された) デジタルデータにワークキーを用いて暗号化を施して暗号化デジタルデータに変換して、データ受信装置へ送信する暗号化手段と、前記ワークキーを得るために必要なコントロールキーを定期的または不定期的に更新生成するコントロールキー更新生成手段と、前記データ受信装置との認証・鍵交換を行う送信側認証・鍵交換手段と、前記コントロールキーを特定できる識別子を生成する識別子生成手段と、前記識別子を前記データ受信装置へ送信する識別子送信手段とを備えたことを特徴とするデータ送信装置。

38. (追加された) デジタルデータにワークキーを用いて暗号化を施して変換された暗号化デジタルデータを受信する受信手段と、

データ送信装置との認証・鍵交換を行う受信側認証・鍵交換手段と、

前記ワークキーを得るために必要なコントロールキーを、前記受信側認証・鍵交換手段を介して得るためコントロールキー取得手段と、

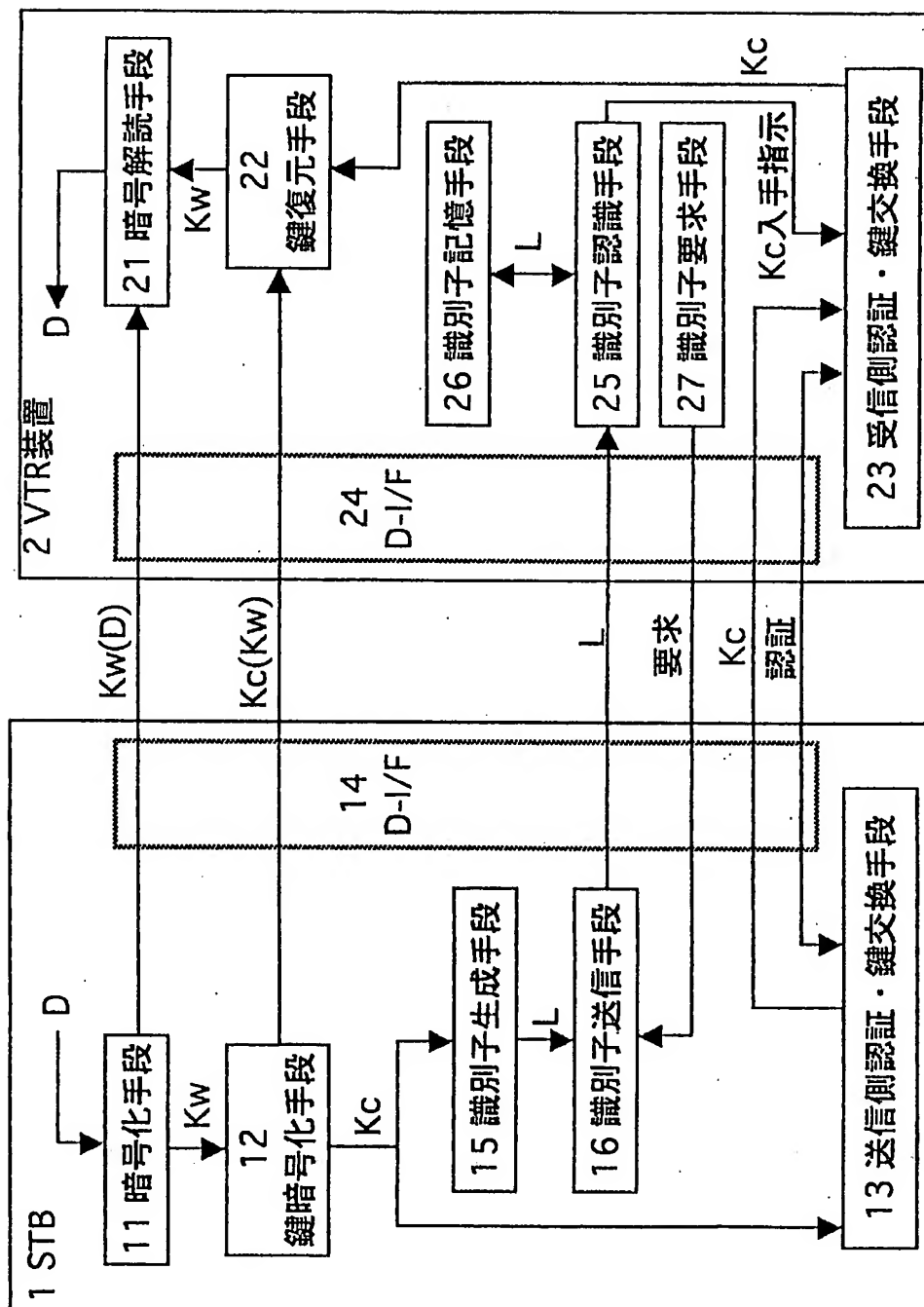
前記暗号化デジタルデータを、前記コントロールキーを用いて生成した前記ワークキーを用いて解読して、前記デジタルデータを復元する暗号解読手段と、

少なくとも、受信中断後に受信を再開する際に、前記データ送信装置から送信されてきた、前記コントロールキーを特定するための識別子を参照することにより、前記コントロールキーが更新されたか否かを判断し、前記コントロールキーが更新されたと判断した場合には、前記受信側認証・鍵交換手段に前記認証・鍵交換を改めて行って更新後の前記コントロールキーを得ることを指示する識別子認識手段とを

備えたことを特徴とするデータ受信装置。

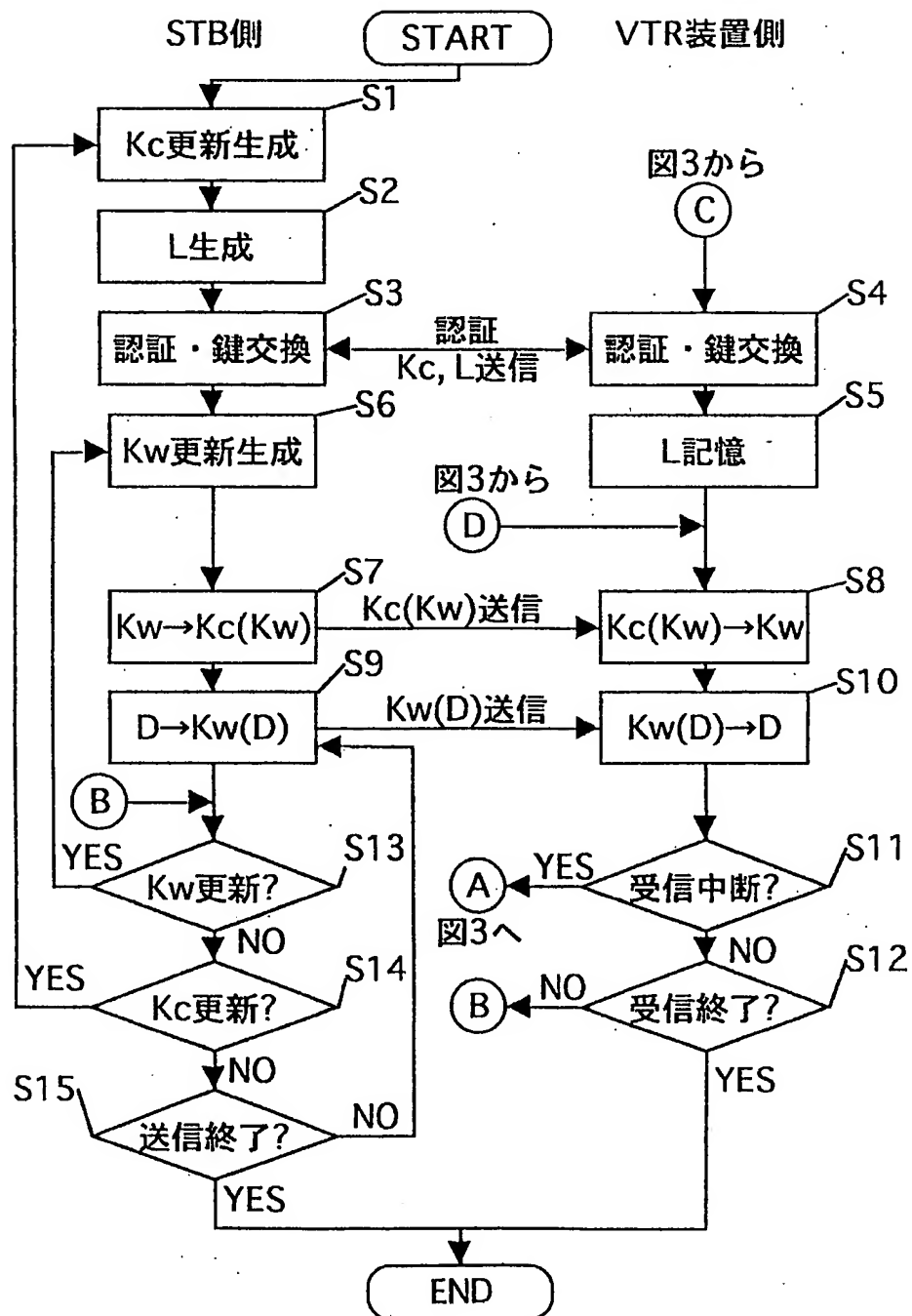
1 / 1 6

第 1 図



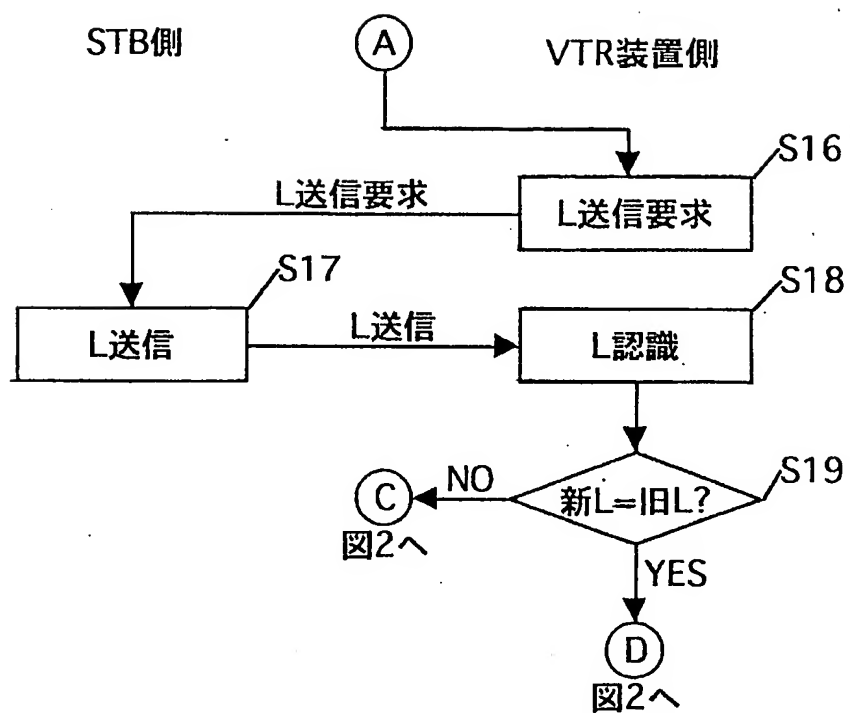
2 / 1 6

第 2 図



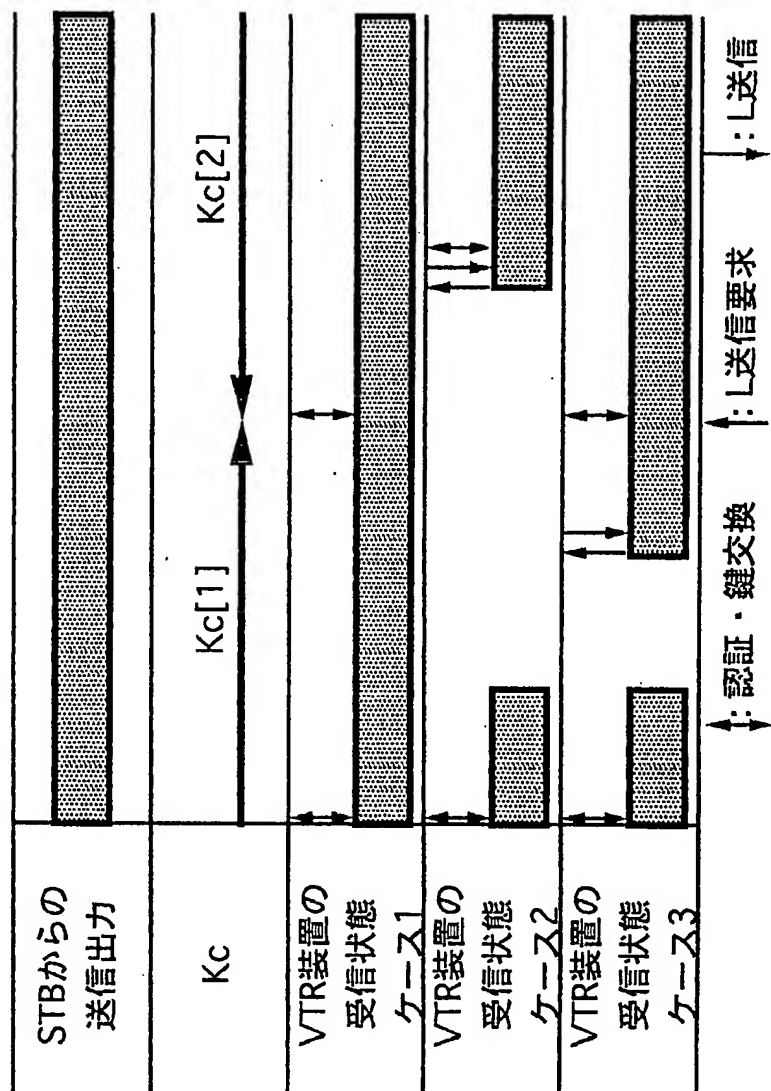
3 / 1 6

第 3 図



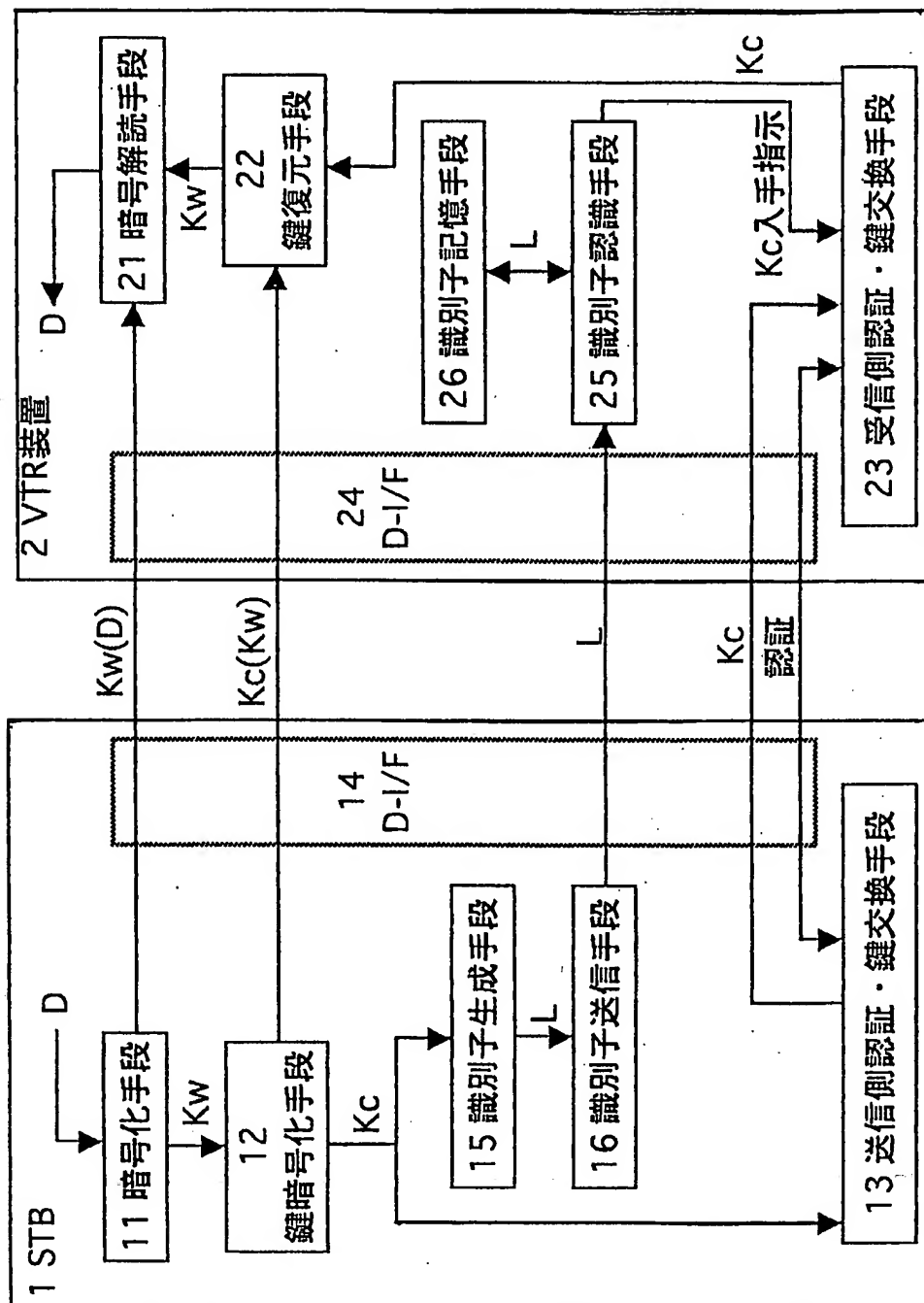
4 / 1 6

第 4 図



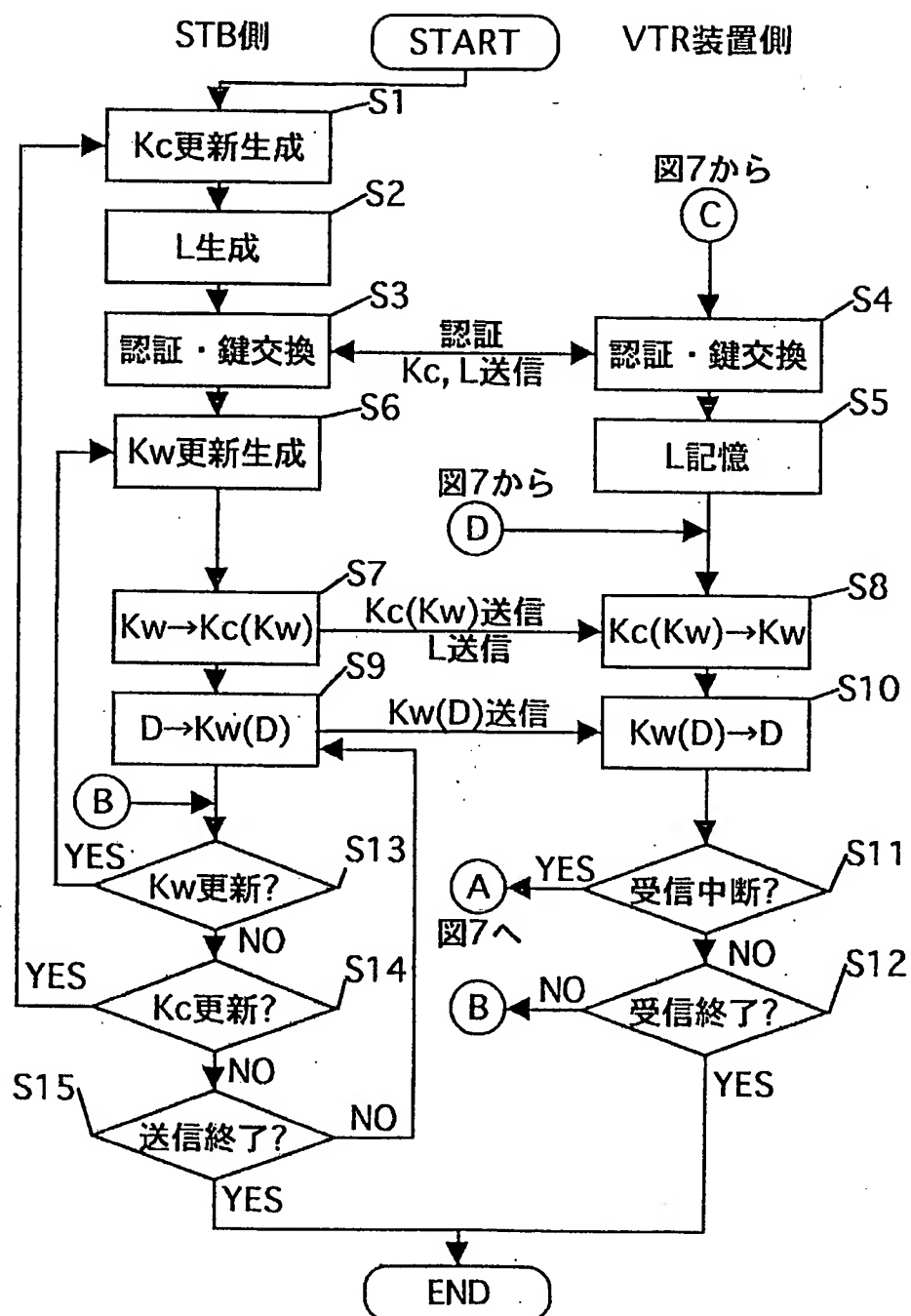
5 / 1 6

第 5 図



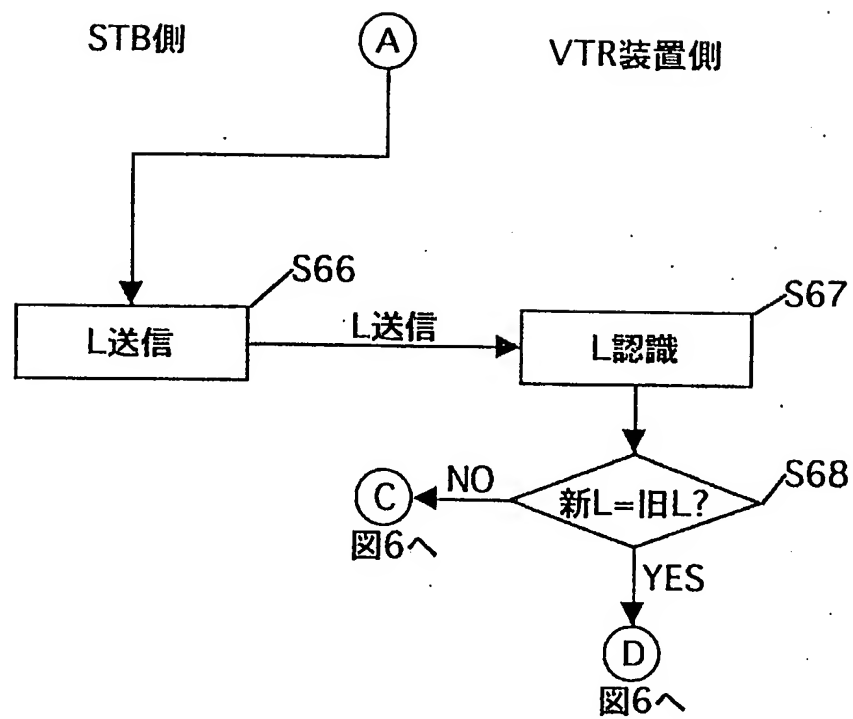
6 / 1 6

第 6 図



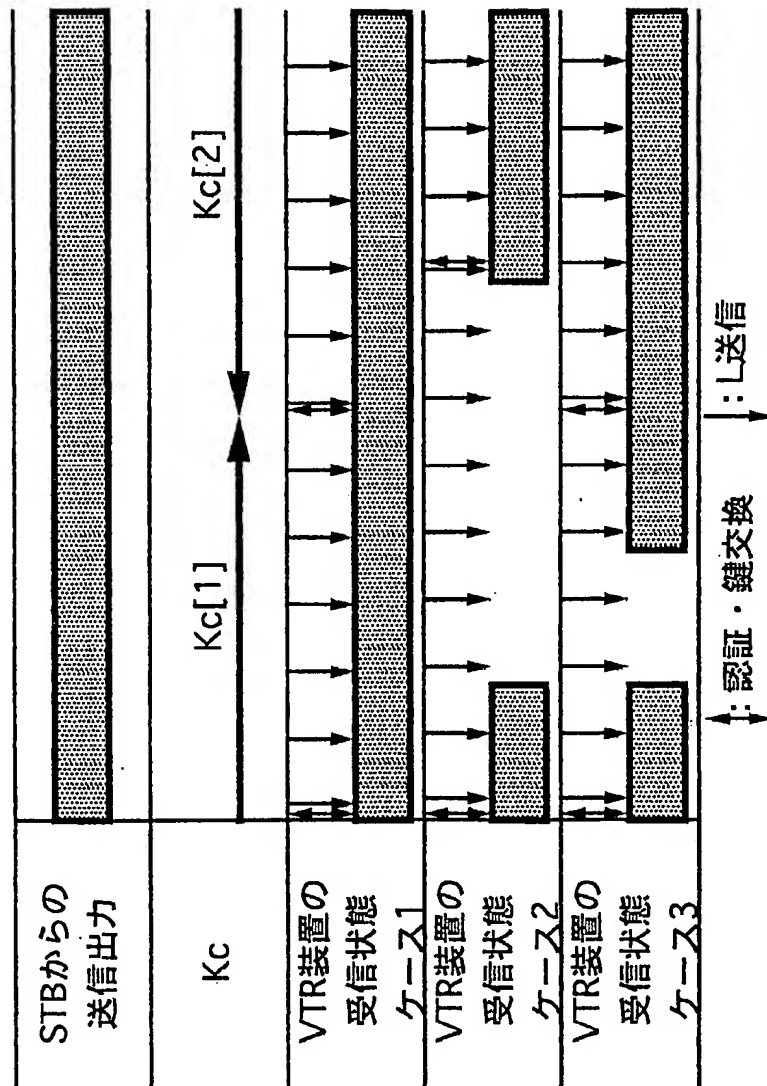
7 / 1 6

第 7 図

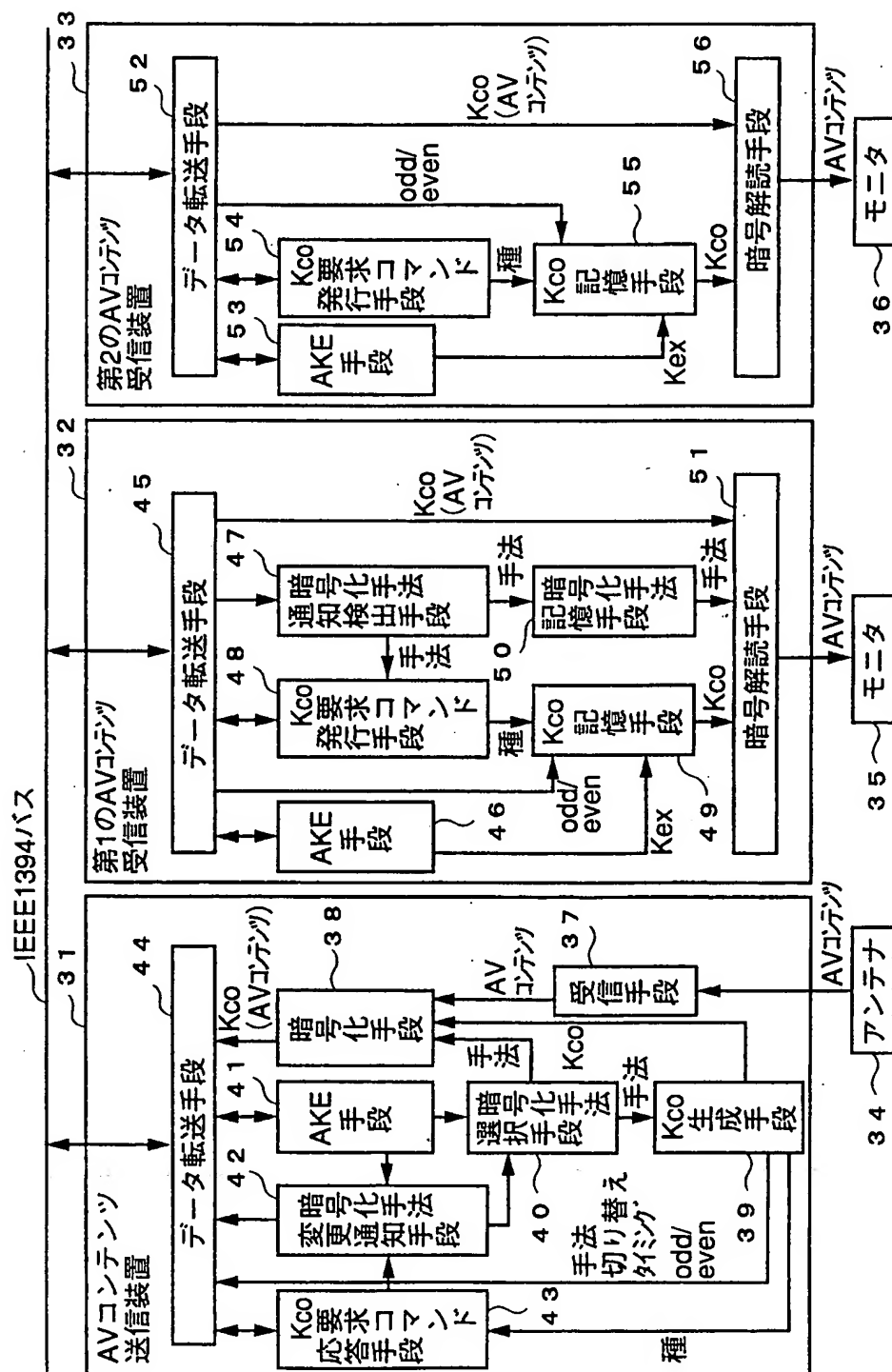


8 / 1 6

第 8 図

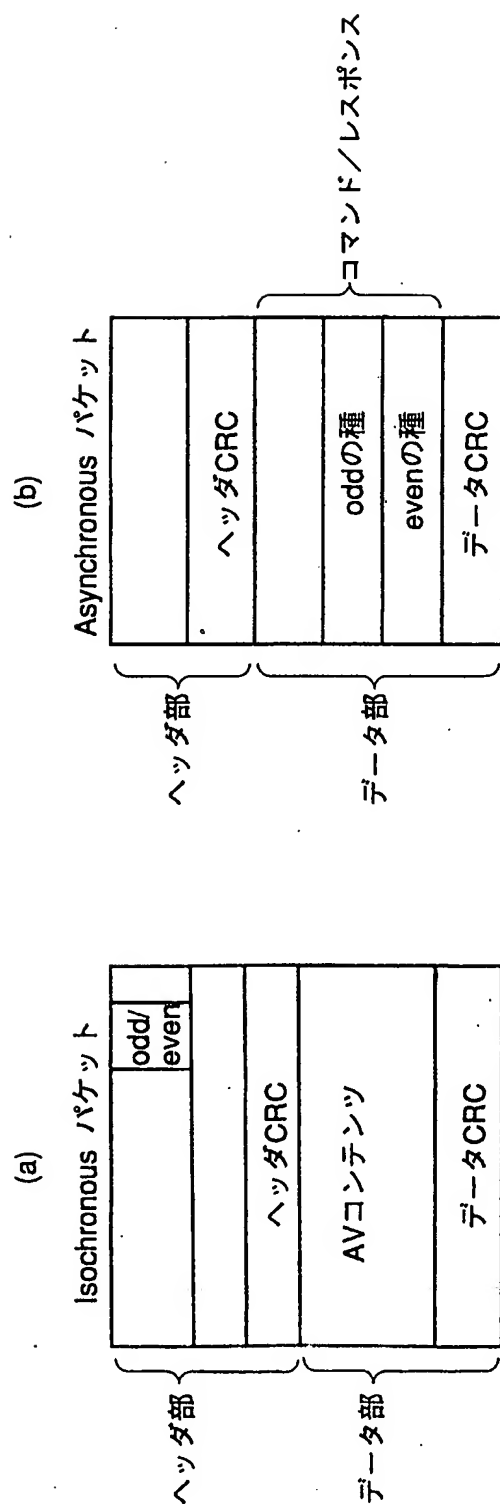


第 9 図



10/16

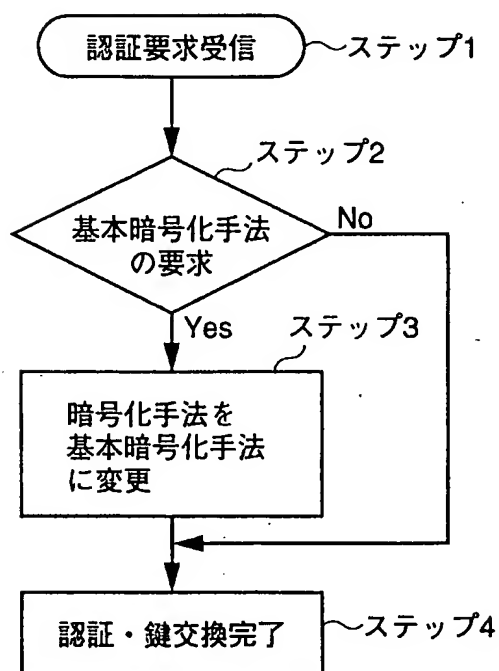
第 10 図



1 1 / 1 6

第 1 1 図

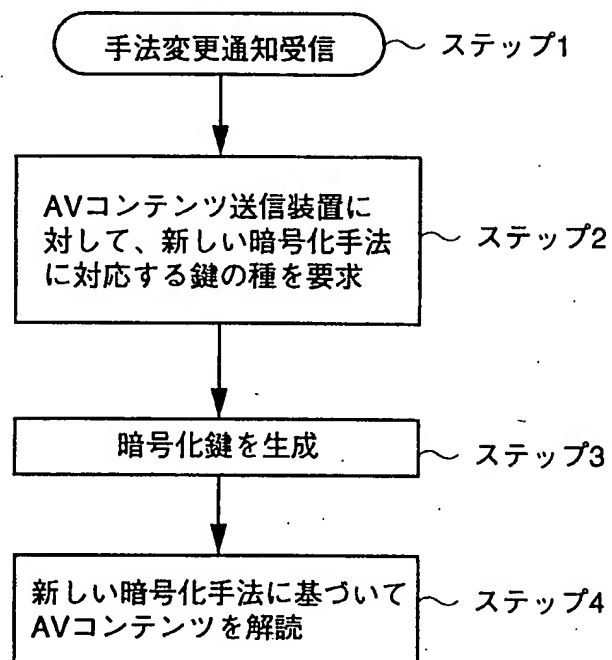
AVコンテンツ送信装置 3 1 の動作



1 2 / 1 6

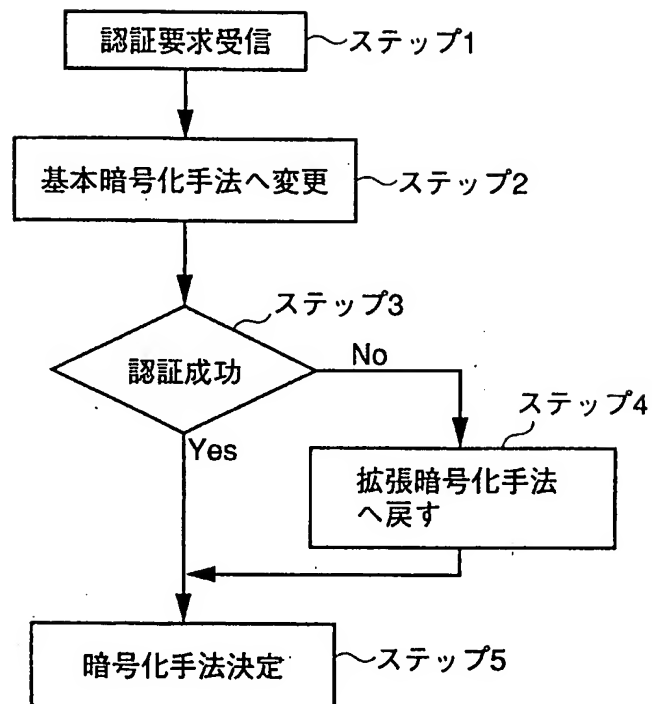
第 1 2 図

第1のAVコンテンツ受信装置32の動作



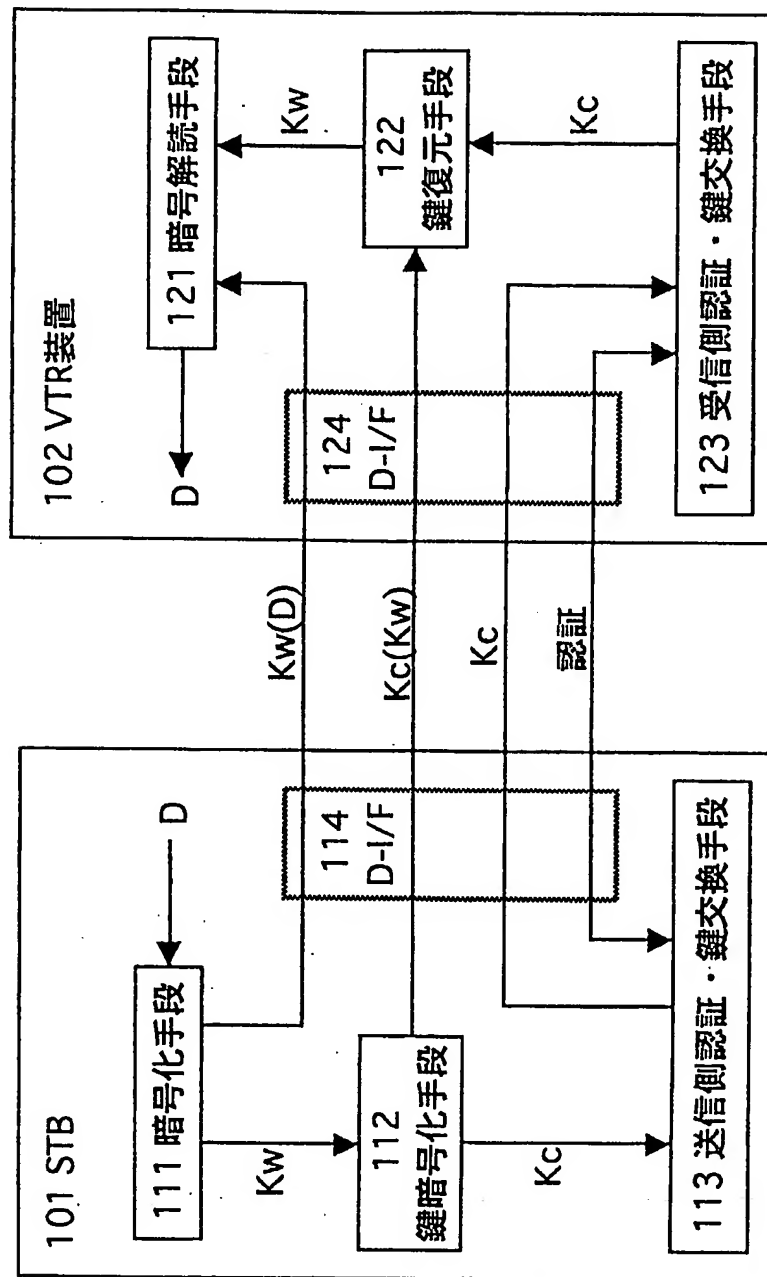
1 3 / 1 6

第 1 3 図



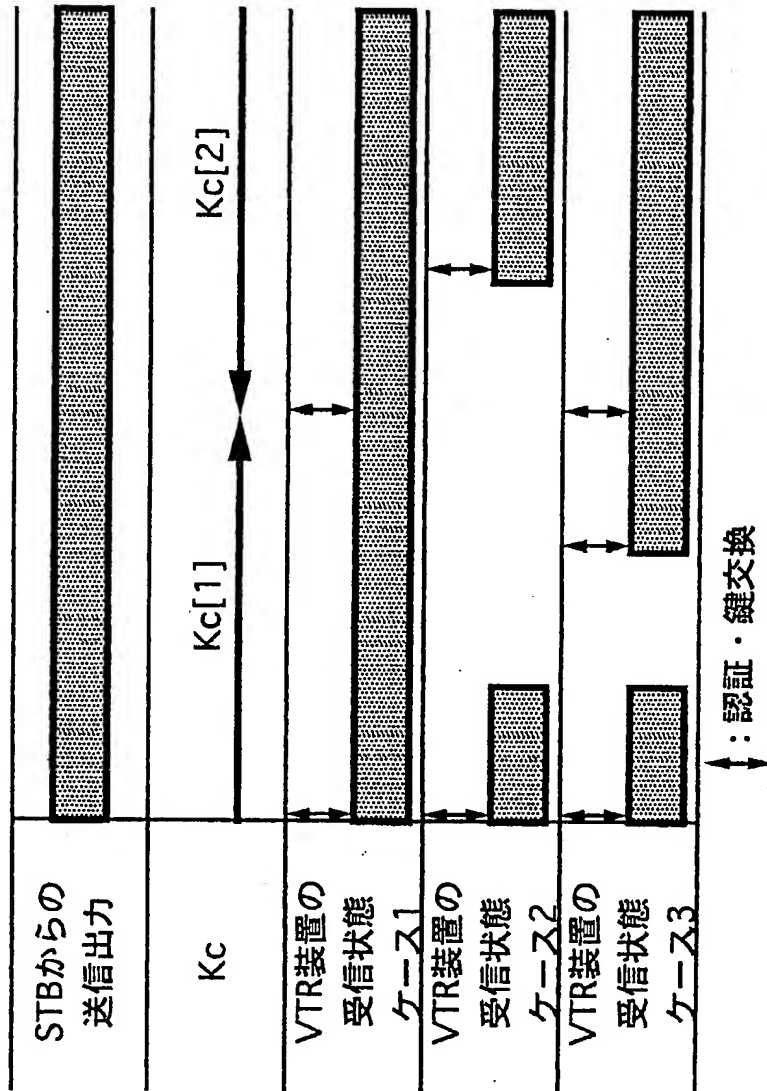
1 4 / 1 6

第 1 4 図



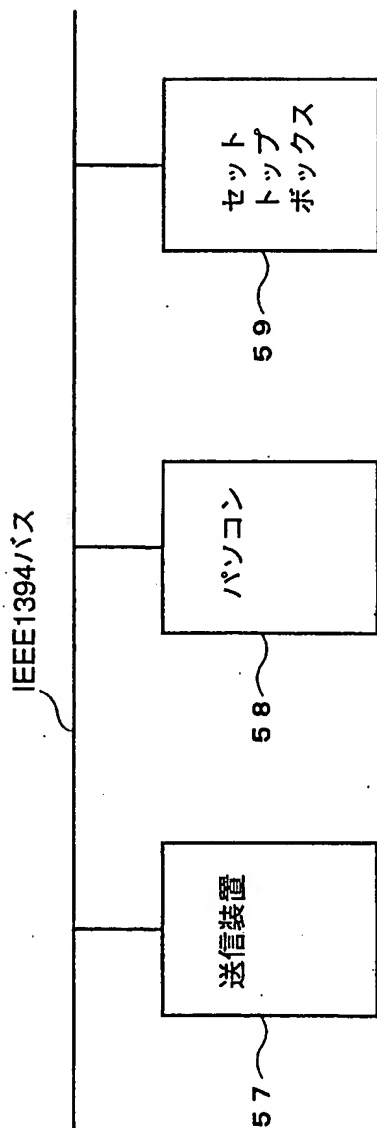
1 5 / 1 6

第 1 5 図



16/16

第16図



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/01606

A. CLASSIFICATION OF SUBJECT MATTER Int.Cl ⁶ H04L9/08, H04L9/14, H04L9/32, H04H1/00		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) Int.Cl ⁶ H04L9/08, H04L9/14, H04L9/32, H04H1/00		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-1999 Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 63-151136, A (NEC Corp.), 23 June, 1988 (23. 06. 88), Full text ; Figs. 1 to 4 (Family: none)	1-15
Y	JP, 9-18468, A (Canon Inc.), 17 January, 1997 (17. 01. 97), Full text ; Figs. 1 to 26 & EP, 751646, A & AU, 9656198, A & JP, 9-16678, A & JP, 9-16679, A & JP, 9-18469, A & JP, 9-46329, A & CA, 2179971, A	16-35
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 13 July, 1999 (13. 07. 99)		Date of mailing of the international search report 21 July, 1999 (21. 07. 99)
Name and mailing address of the ISA/ Japanese Patent Office		Authorized officer
Facsimile No.		Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/01606

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 9-18469, A (Canon Inc.), 17 January, 1997 (17. 01. 97), Page 3, column 3, line 48 to column 4, lines 23, 47 to page 4, column 5, lines 4, 27 to 36 ; page 5, column 7, line 40 to column 8, line 47 ; page 11, column 19, lines 5 to 23 ; Figs. 1 to 17 & EP, 751646, A & AU, 9656198, A & JP, 9-16678, A & JP, 9-16679, A & JP, 9-18468, A & JP, 9-46329, A & CA, 2179971, A	16-35
A	JP, 4-297157, A (Mitsubishi Electric Corp.), 21 October, 1992 (21. 10. 92), Full text ; Figs. 1 to 3 (Family: none)	1-15
A	JP, 59-134939, A (NEC Corp.), 2 August, 1985 (02. 08. 85), Full text ; Figs. 1 to 4 (Family: none)	16-35

Form PCT/ISA/210 (continuation of second sheet) (July 1992).

A. 発明の属する分野の分類 (国際特許分類 (IPC))			
Int. Cl ⁸ H04L9/08, H04L9/14, H04L9/32, H04H1/00			
B. 調査を行った分野			
調査を行った最小限資料 (国際特許分類 (IPC))			
Int. Cl ⁸ H04L9/08, H04L9/14, H04L9/32, H04H1/00			
最小限資料以外の資料で調査を行った分野に含まれるもの			
日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-1999年 日本国登録実用新案公報 1994-1999年 日本国実用新案登録公報 1996-1999年			
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)			
C. 関連すると認められる文献			
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号	
Y	JP, 63-151136, A (日本電気株式会社) 23. 6月. 1988 (23. 06. 88) 全文, 第1-4図 (ファミリーなし)	1-15	
Y	JP, 9-18468, A (キヤノン株式会社) 17. 1月. 1997 (17. 01. 97) 全文, 図1-26 & EP, 751646, A & AU, 9656198, A & JP, 9-16678, A & JP, 9-16679, A & JP, 9-18469, A & JP, 9-46329, A & CA, 2179971, A	16-35	
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。			
* 引用文献のカテゴリー		の日の後に公表された文献	
「A」特に関連のある文献ではなく、一般的技術水準を示すもの		「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの	
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの		「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの	
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)		「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの	
「O」口頭による開示、使用、展示等に言及する文献		「&」同一パテントファミリー文献	
「P」国際出願日前で、かつ優先権の主張の基礎となる出願			
国際調査を完了した日 13. 07. 99		国際調査報告の発送日 21.07.99	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 青木 重徳 印 5W 4229 電話番号 03-3581-1101 内線 3576	

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 9-18469, A (キヤノン株式会社) 17. 1月. 1997 (17. 01. 97) 第3頁第3欄第48行-同頁第4欄第23行, 第3頁第4欄第47行-第4頁第5欄第4行, 第4頁第5欄第27-36行, 第5頁第7欄第40行-同頁第8欄第47行, 第11頁第19欄第5-23行, 図1-17 & EP, 751646, A & AU, 9656198, A & J P, 9-16678, A & J P, 9-16679, A & J P, 9-18468, A & J P, 9-46329, A & CA, 2179971, A	16-35
A	J P, 4-297157, A (三菱電機株式会社) 21. 10月. 1992 (21. 10. 92) 全文, 図1-3 (ファミリーなし)	1-15
A	J P, 59-134939, A (日本電気株式会社) 2. 8月. 1985 (02. 08. 85) 全文, 第1-4図 (ファミリーなし)	16-35

様式PCT/ISA/210 (第2ページの続き) (1998年7月)